网络安全

安全技巧（九）

小未 主编

目　录

浅析网络入侵监测系统-IDS 的应用

很多文章介绍了如何通过建立，改善，以及分析服务器日记文件的种种方式，监测出来黑客入侵行为，但这些都是过去式，都是在入侵发生后你才知道存在这种行为而加以防范。最好的方法是能够在当场就能监测出恶意的网络入侵行为，并且马上采取防范反击措施加以纠正。因此即时监测黑客入侵行为并以程序自动产生响应的网络入侵监测系统（又称 IDS）产生了。

1、何谓 IDS？

简单的说，设立 IDS 的唯一目的就是当场监测到网络入侵事件的发生。IDS 就是一个网络上的系统，这个系统包含了下面三个组件：

（1）网络监测组件，用以捕捉在网络线上传递的封包。

（2）接口组件，用以决定监测中的资料传递是否属于恶意行为或恶意的使用。在网络传递时，用来比较的资料样式 （pattern），以监测恶意网络活动。

（3）响应组件，针对当时的事件予以适当的响应。这个响应可以是简单的，例如寄发一个电子邮件讯息给系统管理者，或者是复杂的，例如暂时将违规者的 IP 地址过滤掉，不要让他连到这个网络来。

2、IDS 如何通过网页监测网络入侵事件

IDS 系统不只必须监测各式各样，从大到小，以及各种系列的系统上的网络攻击事件，它还必须能够快速及时地的在第一时间内监测到入侵事件的发生。因此，I

DS 的数据库以及式样比对（pattern-matching）机制是复杂到令人难以置信的。

要使 IDS 能够监测通过网页的入侵事件，其中的网络监测组件就必须要能够捕捉所有通过网页通讯端口上，借着 HTTP 通讯协议传递的网络资料往来。（注意，SSL 的网络交通是完全绕过 IDS 的网络监测的，因为这些网络交换资料都是经过加密的。）式样比对组件在这里，主要是用于比较 URL 解析的结果，看看是否符合数据库中的恶意的 HTTP 回询（request）。

接下来，我介绍如何制作两个快速而简易的 IDS，用来监测可疑的网页回询活动。这些解决方案的目的是在于提供系统管理者，让他们拥有一个特别针对他们网络而设计的监测/响应系统。

3、制作快速而简易的 IDS

（1）Network Grep 工具

我们先从一个简单的网络监视程序开始，这个程序是用来监测 HTTP 通讯协议的网络资料往来。HTTP 回询的特色是，它使用以下的语法：

〈HTTP-Request-Method〉 〈URL〉 HTTP/〈version〉

这个可在 Packetfactory 入口网站寻获的程序 ngrep 针对在网络上传递往来的资料，执行正则表示法（regular expression）式样比对。我们可以用以下的指令来利用 ngrep 拦截并显示所有纯文字形式的 HTTP 资料往来：

#ngrep-iqt“^GET|^HEAD|^TRACE|^POST|^PUT and HTTP”

以上指令中，-iqt 选项是指示 ngrep 不要区分资料

中的大小写，并且只有显示封包中有符合式样比对的资料，以及在显示资料时加上日期以及时间的标题。（注：比对的式样，是基于 GET，HEAD，TRACE，POST，PUT，以及 HTTP 等关键词。欲知更多有关如何在 ngrep 使用正则表示法，你可以到 http://www.packetfactory.net/Projects/Ngrep/查看相关资料。）

以上面我们建议的方式使用 ngrep 再加上运行越来越受欢迎的 Whisker 程序，监测地址为 10.1.1.2 的 IIS 5.0 服务器平台，我们得到了以下的结果：

T 03:37:30.041739 10.1.1.21:2425 -> 10.1.1.2:80 [AP]

HEAD / HTTP/1.0..User-Agent: Mozilla/5.0 [en]（Win95; U）..Referer: http://10.1.1.2/..Connection: close....

T 2001/01/16 03:37:30.108630 10.1.1.21:2426 -> 10.1.1.2:80 [AP]

GET /cfdocs/ HTTP/1.0..User-Agent: Mozilla/5.0 [en]（Win95; U）..Cookie: ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPBCFD;path=

/..Referer:http://10.1.1.2/..Connection: close....

T 2001/01/16 03:37:31.842452 10.1.1.21:2427 -> 10.1.1.2:80 [AP]

GET /scripts/ HTTP/1.0..User-Agent: Mozilla/5.0 [en]（Win95; U）..Cookie: ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPBCFD;path=

/..Referer:http://10.1.1.2/..Connection: close....

T 2001/01/16 03:37:31.854206 10.1.1.21:2428 -> 10.1.1.2:80 [AP]

GET /scripts/cfcache.map HTTP/1.0..User-Agent: Mozilla/5.0 [en]

（Win95; U）..Cookie: ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPBCFD;

path=/..Referer: http://10.1.1.2/..Connection: close....

T 2001/01/16 03:37:33.644534 10.1.1.21:2429 -> 10.1.1.2:80 [AP]

GET /cfcache.map HTTP/1.0..User-Agent: Mozilla/5.0 [en] （Win95; U）..Cookie: ASPSESSIONIDGQGQGLAC=HDJNBOGBIPOCPNCKOJOPBCFD;path=

/..Referer:http://10.1.1.2/..Connection: close....

现在你就可以采取行动了！

（2）执行式样比对

使用 ngrep **拦截网络资料往来很简单。然而，分析捕捉到的资料并从中抽取** URL **则略具难度。因为** ngrep **将资料输出拆成一行一行的，所以我们必须额外耗费很多精力，去重组输出的资料，并将该资料中的** URL **与已知的网络攻击行为模式做比对。**

此时，我向大家介绍另一个用来监测网页传送的犀利工具软件了。这个软件就叫做 urlsnarf**，它是由** Dug Song **写成的** dsniff **工具软件套件的一部份。**urlsnarf **从所拦截的网络资料传送中，捕捉所有的** HTTP **回询，并且将结果以共享日记文件格式（**Common Log Format , CLF**）显示出来，这种格式就跟市面上的网页服务器，诸如** Apache **或者是** IIS **所用的格式一样。**

跟当初我们用 ngrep **的方式一样，我们使用** urlsnarf **并且在** 10.1.1.2 **的服务器上执行** Whisker**，所得到的**

结果如下：

urlsnarf

urlsnarf: listening on eth0

10.1.1.21 - - [16/02/2001:03:58:43 +0530] "HEAD http://10.1.1.2/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:43 +0530] "GET http://10.1.1.2/cfdocs/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:45 +0530] "GET http://10.1.1.2/scripts/ HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:45 +0530] "GET http://10.1.1.2/scripts/cfcache.map HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:48 +0530] "GET http://10.1.1.2/cfcache.map HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:50+0530]"GET http://10.1.1.2/cfide/Administrator/startstop.html HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

10.1.1.21 - - [16/02/2001:03:58:52 +0530] "GET http://10.1.1.2/cfappman/index.cfm HTTP/1.0" - - "http://10.1.1.2/" "Mozilla/5.0 [en] （Win95; U）"

使用 urlsnarf **唯一的缺点是，它现在的程序是写死的，只监听** TCP **通讯端口** 80**（纯文字** HTTP**），**3128**（**MS-proxy**）以及** 8080**（**generic/squid proxy**）。从其它通讯**

端口传输的 HTTP 协议资料则完全被忽略。要想改变这种限制，你必须在 urlsnarf 的原始程序代码中做一些小小的改变。然而，光是 urlsnarf 所提供的功能，就已经远远的超过它所给我们的限制了。

因为 urlsnarf 以 CLF 格式产生日记，我们可以将它的输出结果，转送到任何在网页服务器上使用 CLF 格式分析日记的日记分析软件。

4、监测恶性入侵性网页浏览行为

通过 urlsnarf 的输出，我们可以开始建立式样比对程序，以寻找网络入侵事件。在这里我利用一个简单的 Perl 程序来跟 urlsnarf 一起监测一些基本的网络入侵行为。我们会把 urlsnarf 的执行结果转传给这个式样比对程序，通过式样比对的方法监测网络入侵行为。

式样比对程序的第一步是，定义一连串入侵性的 URL 查询。为了简单起见，我们只列出某些 URL 如下:

```
%cgis = (
"/msadc/msadcs.dll" => "mdac",
"/msadc/Samples/selector/showcode.asp" => "showcode",
"/cgi-bin/guestbook.cgi" => "guestbook",
"/cgi-bin/test-cgi" => "test-cgi",
"/cgi-bin/finger" => "finger",
"/cfdocs/expelval/exprcalc.cfm" => "exprcalc",
"/cgi-bin/phf" => "phf",
"/scripts/samples/search/webhits.exe" => "webhits",
"/scripts/iisadmin/ism.dll" => "ism",
"/scripts/tools/newdsn.exe" => "newdsn",
"/scripts/perl.exe" => "perl_exe",
"/scripts/proxy/w3proxy.dll" => "w3proxy"
```

）；

我们使用了%cg集中储存所有我们需要的恶意URL查询式样。在这里，我们也可以从一个含有这些“特征”的档案，动态建立这个查询式样库。 注意，以上的URL本身并无害；然而，它们通常被黑客利用来做恶意的网页攻击的基础。（例如：msdacs.dll就可以被用来破坏MDAC/RDS）。

下一步，是设定容忍的最低程度，即：如果某个访客查询某个URL超过三次的话，这个访客的IP地址就会被列在黑名单中。在我们的程序里，定义如下：

```
$threshold = 3;
```

下一段重要的程序代码，是一个以while叙述开始的循环，这个循环会从urlsnarf读取每一个CLF纪录，并且做分析。为了避免谈到太多Perl程序语言的细节，有关 while 循环的说明就像以下这样：

```
while（〈 〉） {
 # # parse incoming log line
 # $logline = $_;
 # # pick out the IP，timestamp andURLfrom the CLFline
 # $logline =~ /（S+）.+?（[.+]）.+?（".+?"）.+/;
 # $ip = $1;
 # $time = $2;
 # $url = $3;
 # # select the resource from the URL
 # $url =~ /w+s+.*//.+?（/.*）s+.*/;
 # $resource = $1;
 # check if there is a match with theURL
```

变量$resource 的值为 URL 回询中的 resource 字符串。例如，如果 URL 为 http://10.1.1.2/msadc/msadcs.dll，那么 resource 字符串的值就是 /msadcs/msadcs.dll。

接着是，寻找我们的 URL“特征”库，看看所查询的 URL 字符串是否符合其中的一个特征。如果式样符合，我们找出这个查询出处的 IP 地址， 然后将它的访客指数加一。如果访客观存在指数超过了我们的容忍底线，那么我们将这个 IP 地址标为黑客地址。

下面是式样比对部分的程序代码:

```
# check if there is a match with the URL
if（$cgis{$resource} ne ""） {
push（@{ $offender_list{$ip} }, $cgis{$resource}）;
# check if the threshold count is crossed
if（$offence_count{$ip}++ > $threshold） {
# response to intrusion detected
print STDERR "** $ip " . join（" "，@{ $offend
er_list{$ip} }） . "n";
} }
```

将这个程序取名为 pattern_match.pl。开始使用 urlsnarf 以及 pattern_match.pl，urlsnarf 以及 pattern_match.pl 得出来的结果应该是如下所示:

```
#urlsnarf| pattern_match.pl
```

一个 Whisker 扫描范例，执行 urlsnarf 以及 pattern_match.pl，监测地址为 10.1.1.2 的 IIS5.0 服务器平台，我们得到了以下的结果:

```
** 10.1.1.21 webhits ism showcode newdsn
** 10.1.1.21 webhits ism showcode newdsn mdac
** 10.1.1.21 webhits ism showcode newdsn mdac
```

w3proxy

** 10.1.1.21 webhits ism showcode newdsn mdac w3proxy perl_exe

这些结果告诉我们，来自 IP 地址 10.1.1.21 的访客为恶意访客，并且也列出了一连串针对 10.1.1.2 的相关可疑的 URL 回询。黑客回报系统是在“特征 URL”已经被查询三次了以后，第四次类似的查询又发生（newdsn）才被激活的。

5、小结

在这里，我向大家介绍了如何利用 IDS 系统监测以网页为媒介的网络入侵活动以及示范如何让各式各样的工具以及 script 在很短的时间内组织起来，以形成功能强大的工具。但由于本人的知识及经验有限，难免存在不足之处，希望大家验给予指正，谢谢！在以后在篇章中，我将会大家介绍网络入侵监测软件如何抵挡黑客们使用的 IDS 躲避技术。

多层次的安全防护系统：让黑客选择放弃

随着网络技术的快速发展和应用的日渐普及，黑客工具不仅变得越来越先进，而且也越来越容易被一般人获取和滥用。黑客技术的提升和黑客工具的泛滥，造成大量的企业、机构和个人的电脑系统遭受程度不同的入侵和攻击，或面临随时被攻击的危险。这就迫使大家不得不加强对自身电脑网络系统的安全防护，甚至追求所谓彻底的、一劳永逸的、100%的网络安全解决方案。

但是，网络安全专家和专业厂商强调，没有一个公

司的安全系统能保证 100%的安全。安全总是相对的。本文阐释的所谓“ 多层次防护 ”, 就是应用和实施一个基于多层次安全系统的全面信息安全策略，在各个层次上部署相关的网络安全产品，增加攻击者侵入所花费的时间、成本和所需要的资源，从而卓有成效地降低被攻击的危险，达到安全防护的目标。事实上，多层次防护已经成为当今网络安全的主流策略。

攻击与防范的互动

网络入侵和安全防范实际上就是指网络攻防技术。攻防技术的此消彼涨始终是网络安全领域前进的动力。攻击技术包括目标网络信息收集技术，目标网络权限提升技术，目标网络渗透技术，目标网络摧毁技术四大类。每一类技术，都是日新月异、不断更新的。所以在网络的安全防范上，我们面对越来越多的新技术的攻击。

在用户方面，不管你是否已经受到这些攻击，不管这些攻击是否产生了比较严重的后果，你都必须假设它们对信息系统的威胁总是存在的。因为一旦你的信息系统受到攻击，你就会蒙受无法估量的损失。在任何时候，对信息系统的连续不断的保护是非常必要的。研究分析表明，单一的安全保护往往效果不理想，最佳途径就是采用多层安全防护措施对信息系统进行全方位的保护。

建设安全保护层

“ 分层的安全防护 ”提供了这样一种思路：结合不同的安全保护因素，例如防病毒软件、防火墙和安全漏洞检测工具，来创建一个比单一防护有效得的多的综合的保护屏障。分层的安全防护成倍地增加了黑客攻击的成本和难度，从而大大减少了他们对企业的攻击。

分层的安全防护技术具体来说包括攻击检测，攻击

防范，攻击后的恢复这三个大方向，每一个方向上有代表性的产品：入侵检测系统负责进行攻击检测，防火墙和强制访问控制系统负责攻击防范，攻击后的恢复则由自动恢复系统来解决。这三大方向就说明了在网络安全防护上的多层安全防护措施。

下面我们就多层次保护中包括的主要环节做具体地说明。

入侵检测系统

入侵检测系统是近年出现的新型网络安全技术，目的是提供实时的入侵检测及采取相应的防护手段，如记录证据用于跟踪和恢复、断开网络连接等。

实时入侵检测能力之所以重要，首先因为它能够对付来自内部网络的攻击，其次它能够减少被黑客入侵的时间。基于主机的入侵检测系统用于保护关键应用的服务器，实时监视可疑的连接、系统日志检查，非法访问的闯入等，并且提供对典型应用的监视。

因此，在提供关键服务的服务器上使用入侵监测系统，安装实时的安全监控系统，可以提高服务器系统的可靠性，使网络安全系统更加强健。选择入侵检测系统，应特别注意其主要性能的情况，包括：协议分析及检测能力；解码效率(速度)；自身安全的完备性；精确度及完整度，防欺骗能力；模式更新速度等等。

入侵检测系统是分层安全中日益被越普遍采用的成分，它将有效地提升黑客进入网络系统的门槛。入侵监测系统能够通过向管理员发出入侵或者入侵企图警告来加强当前的存取控制系统（例如防火墙）;识别防火墙通常不能识别的攻击（如来自企业内部的攻击）;在发现入侵企图之后提供必要的信息，帮助系统的移植。

入侵检测系统虽然已经被越来越被广泛地接受为有效的安全工具，但是有一点非常重要：它不能单独工作。例如，有一种工具软件可以使检测系统失效。这种被称为"Stick"的工具可发出多个有攻击表现的信息包，从而使成为其攻击目标的网络的 IDS 频繁发出警告。结果造成管理者无法分辨哪些警告是针对真正的攻击发出的，从而使 IDS 使去作用。而且，如果有攻击表现的信息包数量超过 IDS 的处理能力的话，IDS 会陷入 DoS(拒绝服务)状态。也就是说：入侵者利用 Stick 模拟大量的虚假的正面攻击来攻击网络中的入侵检测系统。这样入侵检测系统就会试图应付大量的新的攻击。这样会降低入侵检测系统的性能，如果系统不能分辨混在大量的虚假的攻击中的真正的攻击，就可能会导致系统失效。

防火墙

由于入侵检测系统的漏洞的存在，防火墙的就成为多层安全防护中必要的一层。一个防火墙为了提供稳定可靠的安全性，必须跟踪流经它的所有通信信息。为了达到控制目的，防火墙首先必须获得所有通信层和其它应用的信息，然后存储这些信息，还要能够重新获得以及控制这些信息。

防火墙仅检查独立的信息包是不够的，因为状态信息——以前的通信和其它应用信息——是控制新的通信连接的最基本的因素。对于某一通信连接，通信状态（以前的通信信息）和应用状态（其他的应用信息）是对该连接做控制决定的关键因素。因此为了保证高层的安全，防火墙必须能够访问、分析和利用通信信息、通信状态、应用状态，并做信息处理（基于以上所有元素的灵活的表达式的估算）。

安全漏洞评估系统

安全漏洞评估系统是一个漏洞和风险评估工具，用于发现、发掘和报告网络安全漏洞。一个出色的安全评估系统不仅能够检测和报告漏洞，而且还可以证明漏洞发生在什么地方以及发生的原因。它质询网络和系统；在系统间分享信息并继续探测各种漏洞直到发现所有的安全漏洞；还可以通过发掘漏洞以提供更高的可信度以确保被检测出的漏洞是真正的漏洞。这就使得风险分析更加精确并确保管理员可以把风险程度最高的漏洞放在优先考虑的位置。

最新的漏洞评估系统还采用了独特的“路径分析技术”，用以发现漏洞的根本原因。通过分析漏洞的根本原因，任何重复的漏洞、模式或异常的现象很容易被确定到是否是重要问题，或被确定到网络中的系统并且迅速被排除。

防病毒软件

防病毒软件的应用也是多层安全防护的一种必要措施。防病毒软件是专门为防止已知和未知的病毒感染你的信息系统而设计的。它的针对性很强，但是需要不断更新，而且存在一定的片面性。由于这方面的介绍已经很多，这里不作进一步的展开。

多层防护发挥的作用

让我们看看多层防护策略如何发挥作用。

即使网络中的入侵检测系统失效，防火墙、安全漏洞评估和防病毒软件还会起作用。

配置合理的防火墙能够在入侵检测系统发现之前阻止最普通的攻击。

安全漏洞评估能够发现漏洞并帮助清除这些漏洞。

如果一个系统没有安全漏洞，即使某一个攻击没有被发现，那么这样的攻击也不会成功。

即使入侵检测系统没有发现已知病毒，防火墙没能够阻止病毒，安全漏洞检测没有清除病毒传播途径，防病毒软件同样能够侦测这些病毒。

所以，在使用了多层安全防护措施以后，企图入侵你公司的信息系统的黑客要付出成数倍的代价才有可能达到入侵目的。这时，你的信息系统的安全系数得到了大大的提升。

需要特别说明的事，网络安全的多层防护并不是一个空洞的概念和设想，而是当今领先的专业厂商完全可以提供的网络安全系列产品和全面解决方案。如积极倡导并大力实践多层次防护的赛门铁克公司就扮演了一个先行者和领导者的角色。

赛门铁克企业安全系列结合了三种技术之解决方案，包括防毒、过滤解决方案与入侵防护，收购 Axent 之后，更扩展了关于这三方面之各项解决方案。在每一领域中，赛门铁克均不断开发出可以支持主要作业平台(如 Linux,Unix， Windows NT,Windows 2000, Windows Me 等)的各项技术，并在网络上布署多层防护，从防火墙、网络或电子邮件网关口，到服务器或工作站。赛门铁克完成 AXENT 收购案后，开发并推出的内容过滤、电子邮件扫描与入侵防护等应用于多层防护的一系列新技术、新产品。此外，赛门铁克企业安全系列还添加了与 IBM 合作开发完成的数字免疫系统（DIS），并正积极建立全球性的专业服务与安全咨询业务。所有这些，并结合赛门铁克著名之管理工具，包括远程遥控方案(pcAnywhere)、存储方案克隆精灵（Ghost）与中央控管中

心(System Center)，使得赛门铁克能够为企业提供网络安全多层次保护的有效策略和完整方案。

让黑客选择放弃

在结束本文前，我们再回顾一下前面提到的有关网络安全的两个基本认识：100%的安全性是不可能达到的目标；所有问题必须与将牵涉到的风险、成本及效益进行测量比对。实际上，网络安全的多层次防护正是基于这两点认识所给出的对策、方案和承诺。

最近举报率非常高的非法入侵已经很好地阐述了信息战本质上的不平等：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，并影响企业的声誉和业务开展。如果你拥有多层安全防护系统，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。多层安全防护系统使得入侵者更可能放弃对你的系统的攻击。

注意论坛恶意代码

有少数违法捣蛋的人，在论坛里利用恶意的代码在别人的贴子里贴巨型的图片、屏蔽文字导致浏览上的困难，甚至是利用代码造成浏览者死机进行捣乱，严重影响了论坛和网络秩序，搞得众网虫草木皆兵。下面就以国内一个非常著名的财经论坛中一些典型的恶意代码为例，提醒各网民注意，特别是各论坛的维护管理者，请尽快修正自己系统里的技术漏洞，以免让此类事件再次发生。

这个论坛为了方便股民网友之间的交流，也为了不让别的论坛挖掉自己的常客，维持人气，规定在贴子正文里不能放置除了该论坛地址外的任何链接；但是可以在 ID 旁边的 Email 地址栏里放 50 个字节的 HTML 和 JS 代码。问题就是在这里产生的：

只要在 Email 地址中输入一些特殊的代码，就可以改字体颜色(隐文字)比如在 Email 地址中输入 body text =#0000FF 就表示用纯蓝色的字符显示贴子的正文。其中#0000FF 是纯蓝色的颜色代码，#00000 是黑色,#FFFFFF 是白色,也可使用 white,blcak,yellow,red,blue 等代码，如：body text=red 。

如果把字体颜色改为#F1F5F1 色——也就是该论坛贴子的底色，和底色一样，文字就看不见了，即 (这种方法在一个贴里只能使用一次，如果该贴子前面有人已经用过了，你再用就无效了)。这种代码影响的不只是发贴回复的那个部分，而是对全张贴里的正文都有影响。所以用刺激的大红大黄等等颜色代码后，整个屏幕炫目刺眼，浏览该贴的人眼睛会不堪重负，只有放弃。

另外，只要 mail 地址中输入一些特殊的代码，就可以贴图像。代码格式如下：

img src=HTTP://www.XXX.com/XYZ.jpg

其中 src=后面的是图像的网址链接，可以通过在图片上点右键选属性的方法看到。大家很容易猜到，只要链接的这个图片尺寸很大，浏览该贴的速度就会慢得令人无法忍受，从而放弃浏览，也就造成变相的封贴效果。有的人还不只贴一个图。

如果使用下面这个图像地址，会导致 Windows 蓝屏甚至死机，这是 Windows 98 系统的 BUG

img src=c:\con\con

这种造成别人系统死机的行为已经算一种初级的网络攻击。本来是这个论坛里几派不和的圈子之间互相敌对的内部纠纷，（该论坛有一位非常知名的人士，因为频繁地发内容重复的贴和空翻贴刷屏，加上有点吹牛的作风，引起了公愤，他的拥趸和反对者经常破口大骂和贴图封贴互相攻击）但近来有扩散滥用的趋势，连毫不相干的贴也加入恶意代码，殃及无辜。很多人只是来看热闹或是看了贴子的标题，觉得好奇地点击进去，就死机了，如果手头的下载任务还没完成或撰写的文章还没保存的话，损失巨大。

另外，该论坛还有人利用注册机制上的漏洞，用 windows 自动屏蔽不显示出来的代码冒充别人的 ID 进行辱骂、封贴等恶劣行径，应该引起各位版主的高度警惕，引以为鉴。下面对浏览各论坛的普通用户，简单介绍一点防止此类行为后果的方法：

1、如果只是遇到贴里的文字被改变了颜色和尺寸，可以在 IE 的查看选项里，点击查看“源代码”，IE 将会自动打开记事本程序，把该贴转换成 HTML 代码的形式在记事本里。因为记事本是白底黑字的纯文本显示的，不受任何代码的影响，所以浏览其内容没有问题——当然，里面也夹杂了大量的英文 HTML 代码，是定义贴子的网络格式的，你可以置之不理，看中文就行了。这样比正常不方便是肯定的了，只有等论坛的管理员来解决真正的问题了。

2、如果实在是很喜欢你的论坛和里面的网友，要在“风头火势”也上网看贴，为防死机，可以关闭浏览器的图像显示功能：

即选 IE 工具－＞Internet 选项－＞高级－＞把“显示图片”功能关闭，同时还可以不看广告。在需要显示某个图象的时候，可以图像上右键选“显示图象”。

象这个论坛的情况，可能在全国各地都有类似的事情发生，网络管理员应该怎么杜绝此类行为，相信不用我啰唆了，他们都是专业技术人员。BBS 论坛已经在我们的网络生活里占了重要的一席之地，众多的网民在论坛上面找到了老师、朋友甚至是爱人。希望大家都遵纪守法，好好维护这个属于大家的交流场所。论坛的版主和技术人员更是应该认真负责,管理维护好论坛的秩序。

聊天室的攻防技巧

一、简介

随着 Internet 的普及和发展，网络这块净土也被黑客盯上而屡屡出现一些风波，比如重要网站被黑、商务站点受到影响等等，这些事例都是数不胜举。虽然这些事情和我们普通老百姓都是相距甚远的，但还是给网友们带来了不便，要想有效的防护自己的，首先就要知晓对方会采取何种破坏和攻击手段。

实际上存在着许多的聊天工具，比如可以通过 V2 登入到 BBS 进行聊天，也可以通过 IRC 协议进行及时的聊天,比如象 ICQ、MSN 和国内的 OICQ 软件都属于这种形式的聊天。

各种聊天工具都有它们自己的优缺点，比如 IRC 协议因为是完全基于字符的，所以速度比较快。还有网站的聊天，该聊天系统的特点是用户注册登入以后，把用

户浏览页面的情况实时的发送到相关的服务器上,这样，所有在同一个网站上面的用户就可以实时的进行沟通。基于 Web 的聊天服务器系统的最大的优点是完全基于浏览器和 Web 服务器的，所以用户不需要任何其他的客户端的工具，而且由于浏览器完全支持多媒体形式，所以传输的内容可以非常丰富多彩。

二、聊天室存在的攻击行为

我们知道浏览器实际上除了和 Web 服务器进行消息的传送以外，还负责对服务器发送回来的 HTML 页面进行解析，而现在几乎所有的浏览器都支持 JavaScript，这样如果用户在发送信息的时候，不是发送正常的文本而是一些带标记的 HTML 语言甚至是 JavaScript 的时候，如果这些语句又是一些恶意的程序代码，就会对用户造成损害。

另外，用户可以通过代理截获所有发送和接收的数据包，通过自己编写的应用程序不停的向服务器发送类似格式的数据包使服务器不能处理其他用户的信息包，能够这样做的原因是因为浏览器和 Web 服务器通讯并不是通过一个固定的 Socket 连接进行的，服务器端实际上只是判别数据包本身的合法性，并不判断数据包是从哪个 IP 地址和哪个 Port 端口发送的。而浏览器是每次发送数据包的时候和服务器建立一个 Socket 连接，当该次传送完成后连接就会断开。

现在基于 Web 的聊天室有一般有两种形式：一种是需要用户认证的，即用户在登入服务器以前必须进行注册，一种是不需要认证的，即用户只需要用一个 Nickname 就可以登入到聊天室中,只要该聊天室中还不存在这个 NickName 就可以了。关于用户的消息处理，现在几

乎所有的聊天室都关闭了对 HTML 和 Javascript 的支持，或者是仅仅允许一部分用户（比如聊天室的系统管理员等）使用这些功能。

三、需要注意的问题和防范

由于 OICQ 是用户间的直接连接，所以很容易被查出 IP 地址而受到攻击，在解决了单机上的安全问题之后，我们面对的将是如何在网络上进行防护。

首先，建议大家要安装防火墙程序。

目前比较好的防火墙有 LockDown 2000、ZoneAlarm 和天网等等，这些工具都有汉化的版本，因此使用方面应该是没有太大的问题。如果在这些防火墙程序中将安全等级设置为“高”的话，它们就会对网络上发送和接收的每一个字节进行监测，同时也会对指定的端口进行实时的查看，一旦发现有非正常的数据包企图进入计算机系统，它们就会加以拦截。

关于信息长度的限制：

一般来说，在服务器发送给浏览器端的 HTML 中含有的 JavaScript 会对用户输入的信息做检查，防止信息超过一定的长度，但是实际上用户可以不通过浏览器，自己生成数据包发送到服务器端，所以为了防止用户发送过长的数据包，需要在服务器端检查用户的数据包的长度。当然这里同时需要注意的是要在用户登入的时候在服务器端检查用户名称和密码的最大长度，同时如果设定了用户性别的话，也要设定其长度限制，事实上如果用户是通过浏览器方式的话，因为在服务器发送给客户的 HTML 文本中已经通过 JavaScript 剧本做了限定，一般不会有问题，但是要考虑用户通过自己合成数据包发送类似信息所产生的问题。

数据包内容的判断：

因为恶意用户可能会在发送的信息中含有恶意的 JavaScript **代码或者是** HTML **代码，如果这样的信息包在服务器端不经过处理而直接传送到其他用户的浏览器上的话，就会造成其他用户的浏览器不停的打开新的窗口，直到耗尽系统的资源。其他的比如发送特大的图象或者是其他的多媒体文件到指定的客户端就会对该客户端用户造成不良的影响。所以一般我们需要对用户发送的信息进行处理，屏蔽这些** HTML **语句和** Javascript **语句。因为所有的命令都是包含在“** <> **”里面的，所以最简单的方法就是当服务器接收到“** <> **”字符的时候，只把“** <> **”看成是普通的字符而不是命令的标志符，就可以避免这个问题。当然为了增加聊天的趣味性，可以对某一些可信任的用户开放这些功能。**

用户身份的鉴别：

很多聊天室在传送数据包的时候，只是根据网页中隐含的字段得到用户的名称作为用户的标识来发送信息。比如国内比较典型的聊天站点(www.silversand.net)**的用户的发送信息的数据包的格式是这样的：**GET http://chat.silversand.net/BANNER?USER=username&

SAYS=%3Ch2%3Ethis+is+test%3C%2Fh2%3E&IMG=&IMGURL=&

WHOTO=%CB%F9%D3%D0%C8% CB&ACTION=%CB%B5%BB%B0&as=on&msg=HTTP/1.0 **其中** username **就是表示该数据包是这个用户发送的。这样我们就很容易自己构建一个类似的数据包，而把用户名称替换成其他任何我们想要替换的人的名称，这样聊天室中的信息就会变得比较混乱，搞不清楚消息到底是谁发送的。**

为了避免这个问题，我们的解决方案是这样的，当用户首次登入的时候，服务器系统应该生成一个唯一的 sessionID 来标识这个用户，这样，每次用户发送的数据包中必须包括这个 sessionID，服务器根据这个 sessionID 来识别是否是该用户发送的消息，如果是一个不合法的 sessionID 的话，就简单的丢弃这个数据包。因为 sessionID 是在服务器端随机生成的，所以用户很难自己构造一个合法的 sessionID 来欺骗服务器，保证了信息来源的可靠性。当然如果服务器需要用户首先注册的话，可以同时检查用户的密码和 sessionID 是否匹配，这样用户伪造其他用户的信息的可能性就会更小。

关于用户发送重复的信息和自动循环发送随机信息（即通常所说的聊天室刷屏现象）的处理：

如果用户只是通过浏览器操作的话，服务器传送给用户的 HTML 文本中包含的 Javascript 就会在用户发送消息的时候比较用户的本次信息是否和上次信息相一致，如果是相一致的话，系统就不会发送本次信息并给出警告。而且如果用户是在浏览器上进行操作的话，用户的信息发送间隔会受到手工操作的限制。但是，如果用户是通过自己的应用程序发送数据包的话，就不会有这个限制。实际上用户可以在一个线程中不断对服务器循环发送数据包。所以系统不仅要考虑在客户端有这个限制，还需要在服务器端进行限制。

我们的解决方案是这样的，对所有在线的用户，我们建立了一个用户池，它实际上是一个用户对象的链表，每一个用户对象包含了用户的名称，用户的 sessionID，用户的上一句发言的信息和用户上一句发言的时间。实际上这个用户池也是滚动的，如果用户在最近一段时间

内没有任何信息，我们就认为该用户已经不在线上，就从信息池中删除该用户，以便为其他用户的连接让出资源。如果用户发送的消息和上一次消息相同的话，就简单的丢弃用户的这个数据包，如果用户这次消息的发送时间和上一次时间间隔小于一定范围（比如一秒）的话，我们就认为这种数据发送速率是非正常的，就简单的从用户池中删除这个用户，断掉这个连接。通过这种解决方法有效的解决了用户刷屏和发送重复消息的问题。

四 小结

本文介绍了 Internet 的聊天系统和不同的特点，重点介绍了聊天室存在的问题和一些攻击行为的防范，虽然黑客猖獗，不过胜利始终是属于正义一方的。

将病毒斩草除根

电脑，提高了我们的工作效率，丰富了我们的生活，但与此同时，电脑病毒也给我们带来了无穷的烦恼。电脑一旦感染了病毒，如果是一般的，只需凭借市面上的杀毒软件就可三两下将其“摆平”，但要是碰上了那些难以对付的病毒就没那么好办了，有时，你虽然对病毒深痛恶极，但你机器上的杀毒软件却“心地仁慈”，往往点到即止，手下留情，不忍将其赶尽杀绝，结果，大部分的病毒是给赶跑了，但小部分的病毒还恋着不走，在那里“生儿育女”。这时，你是望毒兴叹呢还是欲将其彻底消灭、斩草除根而后快？我想你肯定会选择后者，那么，怎样才能做到这一点呢？

1、用多个杀毒软件轮流杀毒。

由于不同种类的杀毒软件自身侧重点不同，各有所长，也各有所短，因此最好多个杀毒软件轮流进行查杀，这样一来，不但可以扬长避短发挥各自软件的优势，而且还可以交叉查杀病毒，效果特佳。我的电脑在一次感染病毒后，开始也是只用一个杀毒软件去杀的，但杀来杀去都杀不彻底，后来就用瑞星、金山毒霸、行天 98 轮流进行查杀，结果才将它彻底地消灭掉了。

技巧 :到网上去下载多个共享或试用版的杀毒软件，这么一来不但可省些银子，而且由于它们都是作为样板供大家使用的，所以效果并不会比购买的差，不过有些是有使用的期限的，如金山毒霸，试用期是 30 天。另外，下载时应注意到正规的网站上下载，下载后应查一查毒，还要注意有无冲突，运行稳不稳定等。

2、认真做好杀毒软件里的各项设置。

通常，一个杀毒软件在首次运行时，其默认的杀毒设置是不能符合我们的需要的，所以，我们必须因“ 毒 ”制宜对它进行相应的设置：

⑴、当你不能确定病毒的性质时，应在“ 查杀设置 ”中选中“ 所有文件 ”, 包括“ 查压缩文件、包含子文件夹、查未知宏病毒、清除未知宏病毒（所有宏）”等，这样，查杀才能更为充分广泛和深入，避免漏杀。

⑵、如果你已知道了该病毒的性质，则应有选择地做好各方面的设置，如你已知道了你的电脑感染的是‘ 欢乐时光 ”的话，则只需查杀“ htm、html、htt、asp ”的文件就可以了。这样不但可加快查杀病毒的速度（这样的设置对于一些电脑里有大量的文件来说特别适合），而且可避免杀伤一些容易杀伤的文件，如 WORD 文件，造成不必要的损失，而如果你怕这样做会造成漏杀的话，

可先用多个杀毒软件用此法轮流查杀后再对所有的文件进行一次全面的“扫荡”。

3、用干净的磁盘引导系统，在 DOS 模式下进行杀毒。

在 Windows 的环境下杀过之后，还要在 DOS 模式下进行查杀，这样才可以更彻底地清除掉电脑上的病毒。现在，许多人都只注重在 Windows 操作系统上杀毒，杀过后就算了，忽视了在 DOS 模式进行清杀的重要性。事实上，很多病毒和中毒较深的电脑是必须在 DOS 模式下才可以清除干净的，尤其是引导型病毒。因此，当你在 Windows 环境下杀过毒后，别忘了再在 DOS 模式下杀一遍。

技巧：一般的杀毒软件，都可以不用任何的人工干扰就可以直接用磁盘在开机后进入到 DOS 模式下杀毒，但对于某些在网上下载的杀毒软件来说则未必如此，有些要你在安装时自己制作杀毒盘，并且通常不能直接自动进入到 DOS 模式下杀毒，这时就要你自己找到该杀毒盘的杀毒程序文件在 DOS 模式下作为命令来启动它了，那怎么找呢？方法如下：

㈠、将一张已制作好的用于 DOS 环境下杀毒的软盘放进软驱。

㈡、在 Windows 环境下进行杀毒测试。

⑴、先在 Windows 中打开该软盘，然后再从“开始－程序－MS-DOS 方式”打开 DOS 窗口。

⑵、将鼠标移至任务栏并按下右键，在弹出的快捷菜单中选择“横向平铺窗口”或“纵向平铺窗口”并单击，以便能同时在 A 盘窗口和 DOS 窗口两个窗口中工作。

⑶、在打开的软盘文件中看看有哪些最尾的字样为“EXE”的文件(即扩展名为EXE的程序文件)，并将它作为命令输进MS－DOS窗口，再看看它能不能被启动并查杀病毒，如果不能就再找下一个这类的文件测试，直到找到为止，找到并经测试后确认它能被运行就可以确定它是杀毒引擎的文件了，然后按“ESC”键停止该程序的运行，再将该杀毒引擎的文件名用笔抄下来，作为在纯DOS下杀毒的命令，最后关闭MS－DOS窗口。注意：有些杀毒软盘不支持在Windows环境的DOS模式下杀毒，如瑞星2001标准版，这时，在找到该杀毒引擎的文件后它会给出提示，这样也同样可以确定它是杀毒引擎的文件。

㈢、进入纯DOS环境后进行杀毒。在纯DOS模式下进行杀毒和在Windows环境的DOS模式下进行杀毒测试时启动杀毒引擎所需输入的命令是一样的。

4、运用手工杀除该病毒的原理进行检查，看看是否还有该病毒存在。

如果是那些难以根除的病毒，尽管你用了以上的方法去杀，也很难杀干净，我的电脑感染了欢乐时光病毒后就是如此，这时应怎么办呢？首先，你要删除所有能感染但不重要的文件，如欢乐时光容易感染的文件主要是“htm”或“htt”、“asp”类文件，这些多数是网页类文件，不是很重要，我的电脑在感染此病毒后我就删除了所有IE里的“历史”文件和OE里的E－MAIL，接着，你就要想方设法获得用手工杀掉该病毒的方法，然后再灵活地运用这个原理来搜索还有没有文件带有该病毒。例如，据资料介绍，用手工杀掉欢乐时光病毒的方法是先查出所有的“htm”或“html”、“htt”、“asp”的

文件，看看它们的源文件中是否含有“ Rem I am sorry! happy time ”，如果有，则表明该文件染上了欢乐时光，将该文件删除。其实根据这个方法，我还可以用它来查电脑里是否还存在欢乐时光病毒。

技巧：杀完毒后，检查你的电脑是否还有病毒存在可用“ 开始/查找 ”的“ 查找 ”程序来检查，这样会更省时省力。方法是：

①、获得病毒所特有的特征编码（一般的病毒都有），如欢乐时光的特征编码是：带毒文件的源文件中含有“ Rem I am sorry! happy time ”。

②、将这些特征编码输入“ 查找 ”程序的“ 包含文字 ”里后开始查找。

③、如果能查到有这类的文件，再看看它们被修改过的时间，如果是近期的，则极有可能是带毒文件。

④、按不同病毒的检查方法进一步确定其是否为带毒文件。

用此法检查可省去检查大量相关文件的麻烦，可大大提高工作效率，而且检查结果准确，一般来说，你电脑上所有带有该病毒编码的文件都能用此方式搜索出来（这种技巧是我后来悟出来，并经反复试验后证实可行，它比起《彻底消灭“ 欢乐时光 ”》一文中的检索病毒文件的方法又先进了许多）。

5、用手工删除用以解释、运行该病毒的程序文件。

如果用尽了所有的办法都不能彻底地将病毒消灭掉的话，最好在不影响重要的程序执行的情况下，“ 宁杀一千，不漏一个 ”，将用以解释、运行该病毒的程序文件删除。例如，用以解释运行欢乐时光病毒的是 WScript.exe 和 JScript.exe，在确定了用尽所有的方法都难以彻底地

将它消灭掉的情况下，就将它们删除掉。如果删除某些程序文件后使某些你要用的程序不能运行，则可在彻底消灭病毒、确认病毒不再有复发的可能后再重装被破坏的程序或系统。

6、注意事项：

⑴、不要过于相信专家的话。

我的电脑感染了欢乐时光病毒后，我看了篇很权威的文章，说只有“ htm ”、“ htt ”、“ html ”、“ asp ”这类文件才会染上该病毒的，但经过我手工的检查后，却发现在“ 已删除邮件 ”的这个“ .dbx ”类的文件里头也带有欢乐时光病毒(这是因为它含有 E－MAIL 文件的缘故)，而且发现后我再用三个杀毒软件轮流来查都不能查出病毒来。

⑵、在用多个杀毒软件杀毒时应注意：

不能多个杀毒软件同时工作，否则由于它们之间不兼容而容易造成死机甚至开不了机,我就曾有过这经历，那时差点搞得整个系统都崩溃了。正确的操作方法是用一个杀毒软件杀完后立即将它关闭（但不用御掉，装了不用一般不会产生冲突)，再用另一个来杀，轮流着来。

⑶、杀毒不能过于频繁。

如果一天连续几十个小时都在杀毒话，则可能毒还没杀光电脑的硬盘却给你杀坏了，我有个同学就曾有过这样的教训。

⑷、如果你不知道用手工查杀该病毒的方法，不要认为这需要很多专业的知识才能做到。

在你已知你的电脑是感染了何种病毒的情况下，只需到一些杀毒方面的专业网站或是“ 瑞星、金山毒霸、KV3000 ”等杀毒软件的网站去找找，一般都可找到相关

的资料。

⑸、如果你怕杀毒软件杀坏你某些重要的文件的话可用杀毒软件先查毒，待查出是否有病毒或是何种病毒后再作进一步的处理。

如查出是“欢乐时光”病毒后我们只需对相关的文件进行杀毒就可以了，这样不但可避免杀伤一些容易杀伤的不相关的文件，而且可加快查杀病毒的速度。如果你有相关的专业知识的话还可用手工进行杀毒，这样就更为安全了。

⑹、请专业人士指导。

如果你用尽了所有的办法都不是病毒的“对手”，则可到一些杀毒方面的专业网站，找到他们的站长的 E－MAIL 地址、OICQ 号码，向其请教，也可以在其论坛或一些综合门户网站的电脑病毒方面的论坛上贴贴子，还可以 E-mail 给你所使用的杀毒软件的厂商，请他们帮你解决。

小心邮件中改头换面的嵌入对象

谁都知道,附件病毒为了迷惑警惕性不高的人,往往摆出一个假的常见后缀名的姿态。如：*.TXT.VBS,*.GIF.EXE 等。EXE 文件还可以在图标上做文章，但是 VBS 文件总是会露出狐狸尾巴，因为它的图标一见便知。这种伎俩毕竟是变形不成功的猪八戒，明眼人是不会上当的。我这里要说的是 OutLook 中存在一种图标及后缀名达到完全隐身但其本身又是可执行的嵌入对象，极易被人利用，请大家注意辨识，下面我以 OouLook2000 简体

中文版为例进行详细说明。

1．开启 OutLook2000，新建一个邮件，选择菜单[格式]/[带格式文本]，在邮件正文点击一下鼠标左键，选择菜单[插入]/[对象]/选择[由文件创建]/[浏览]选择 WINDOWS 目录下的 NOTEPAD.EXE /[确定]，在新邮件的主体部分出现 NOTEPAD.EXE 及其图标。

2．在刚出现的 NOTEPAD.EXE 及其图标上点击鼠标右键，选择[编辑包]，打开对象包装程序，选择[插入图标]按钮/选择[浏览]/选择 WINDOWS\SYSTEM\SHELL32.DLL/在当前图标框中选择一个你想要的图标,我选择的是文本文件的图标，然后按[确定]。当然在这一步图标的选择余地非常大。然后选择菜单[编辑]/[卷标]/任取一个名字,我取 JOKE.TXT/选择[确定]。

3．退出对象包装程序，在提示是否更新时选择[是]。

4．OK，现在出现在面前的是 JOKE.TXT,一般人会认为它是一个地地道道的文本文件附件，相信没有人怀疑它是别的东西。请你双击这个图表，看看会发生什么？是不是发现它打开的是 NOTEPAD 如果它是一个病毒可执行文件，结果可想而知。

当你用 OutLook2000 收到这样一个邮件时,它会显示这是一个带附件的邮件，当你以为它是一个文本文件附件双击打开时，OutLook 会提示：部分对象携带病毒，可能对你的计算机造成危害，因此，请确保该对象来源可靠。是否相信该嵌入对象？安全观念强的人一般会选择 NO,一般的人可能会选择 YES。

不要怕，尽管它的迷惑性极大，但是仍然会露出一些马脚：

1．它其实是一个 OLE 对象，并不是附件，选择它

时，选择框会不同于选择附件的选择框。点鼠标右键出现的菜单不同。

2.双击打开它时,安全提示与附件的安全提示不同，这点非常重要。这时，因该选择 NO，然后点击鼠标右键，选择[编辑包]，提示是否信任该对象时选择 YES，在对象包装程序的右边内容框中，将现出原形。我这个例子中，会显示“ NOTEPAD.EXE 的备份 ”。文件是否可执行，关键在这里。

3．因为它不是附件，在选择[文件]/[保存附件]时并无对话框出现。

因为并不是所有的邮件收发软件都支持对象嵌入，所以这类邮件的格式不一定被某些软件识别，如 OutLook Express。但是 OutLook 的使用面很广，尤其是在大的有自己 MAIL 服务器的公司，所以还是有必要提醒大家小心嵌入对象，不光是 OutLook，其实 WORD，EXCEL 等支持嵌入对象的软件可以让嵌入对象改头换面以迷惑人。

Windows 2000 漏洞集锦

登陆输入法漏洞

这里我们首先介绍一个登录错误，也就是常说的输入法漏洞。当我们启动 Windows2000 进行到登录验证的提示界面时,任何用户都可以打开各种输入法的帮助栏，并且可以利用其中具有的一些功能访问文件系统，这也就是说我们可以绕过了 Windows2000 的用户登录验证机制，并且能以最高管理员权限访问整个系统。所以说

这个漏洞的危害性是很大的，而且当我们进入系统后，还可以利用 Terminal Server 远程通信这个漏洞对系统进行攻击。默认的 Windows2000 系统自带的输入法中有这个漏洞的是：智能 ABC,微软拼音,内码,全拼,双拼,郑码。所以就我感觉而言这个漏洞是首要修补的漏洞。

1、把不需要的输入法删除掉，例如郑码等。

2、但是毕竟我们不能把所有的自带输入法都删除，如果我们要使用有漏洞的输入法也可以把那个输入法的帮助文件删除掉。这些帮助文件通常在 win2000 的安装目录下(如:C:\WINNT)的\help 目录下，对应的帮助文件是：

※ WINIME.CHM 输入法操作指南

※ WINSP.CHM 双拼输入法帮助

※ WINZM.CHM 郑码输入法帮助

※ WINPY.CHM 全拼输入法帮助

※ WINGB.CHM 内码输入法帮助

3、微软公司对于此问题发布了 MS00-069 安全公告，并在互联网上给出了简体中文 Windows2000 和英文版 Windows2000 的补丁。所以请尽快打上补丁。

NetBIOS 的信息泄漏

接下来我们谈一下 NetBIOS 的共享入侵.这个问题从 NT 刚发行到现在就从来没有解决。而且它一直由来都是 NT 系统构架最常见的入侵手段。特别值得一提的就是那个 IPC$Null session(空会话)在 NT 系统里都是已知的安全隐患。虽然打了 SP3 后可以通过修改注册表来对其进行限制。但不知道为什么 Windows2000 还是原封不动地保留着这个空对话。那么就让我们来看看空会话能给入侵者带来什么样的信息：

net use \\server\IPC$ "" /user:""//**此命令用来建立一个空会话**

net view \\server//**此命令用来查看远程服务器的共享资源**

服务器名称注释

\\pc1

\\pc2

命令成功完成。

net time \\server//**此命令用来得到一个远程服务器的当前时间。**

nbtstat -A server//**此命令用来得到远程服务器的** NetBIOS **用户名字表**

NetBIOS Remote Machine Name Table

NameTypeStatus

NULL <00> UNIQUE Registered

NULL <20> UNIQUE Registered

INTERNET <00> GROUPRegistered

XIXI <03> UNIQUE Registered

INet~Services<1C> GROUPRegistered

IS~NULL.....<00> UNIQUE Registered

INTERNET <1E> GROUPRegistered

ADMINISTATOR <03> UNIQUE Registered

INTERNET <1D> UNIQUE Registered

..__MSBROWSE__.<01> GROUPRegistered

MAC Address = 00-54-4F-34-D8-80

看看，只不过用了几个系统自带的命令就得到了如

此多的信息，那么我们有什么办法可以不让别人轻易得到这么多信息哪？

仅靠单纯的修改注册表是一劳永逸的。

HKEY-LOCAL_MACHINE\SYSTEM\CurrentContro Set\Control\LSA

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Value: 1

但如果一些服务你并不需要开放共享的话。那为什么不禁止它呢？在 Windows2000 里的方法和 NT4 的略有不同。它没有限制 TCP/IP 绑定在 NetBISO 上，但是我们可以在 Internet 协议(TCP/IP)属性的设置面板里选取高级(V)选项，然后选择 TCP/IP 筛选，接着点选启用 TCP/IP 筛选，最后在 TCP 端口点选只允许，然后就可以添加你所想开放的服务的端口了。

奇怪的系统崩溃特性

此外 Windows 2000 有一个比较奇怪的特性，使用系统的终端用户可以通过按住右 Ctrl，同时 Press 两次 S crool Lock 按键，就轻易可以让整个 Windows2000 系统完全的崩溃。但同时又在 C:\WinNT\下 dump 完整的当前系统内存记录，内存记录文件名是 memory.dmp。当然，这个奇怪的特性默认状态下是关闭的，但是我们可以通过修改注册表的方法把它激活：

1、运行 regedt32.exe （Windows2000 的 32 位注册表编辑器）

2、选择主键：

HKEY_LOCAL_MACHINE\

然后找到 SYSTEM\下的 CurrentControlSet\

选择 Services\

进入 i8042prt\中的 Parameters

3、新建一个双字节值

4、将键名为 CrashOnCtrlScroll

5、然后在设置一个不为零的值。

6、退出重启

当这一切做完后，你就可以尝试让系统崩溃了，按下按键后的效果为黑屏，将会出现以下信息：

*** STOP: 0x000000E2 (0x00000000,0x00000000, 0x00000000,0x00000000)

The end-user manually generated the crashdump.

值得注意的是，这个奇怪的特性在 WindowsNT4 中也存在,不知道是不是微软程序员作测试的一个小功能。不过要是有黑客或者病毒利用它，也是很危险的。

Telnet 的拒绝服务攻击

Windows 中的 Telnet 一直以来都是网络管理员们最喜爱的网络实用工具之一，但是一个新的漏洞表明，在 Windows2000 中 Telnet 在守护其进程时，在已经被初始化的会话还未被复位的情况下很容易受到一种普通的拒绝服务攻击。而在 2000 年的 2 月份，拒绝服务攻击几乎成为了所有大型网站的恶梦。

Telnet 连接后，在初始化的对话还未被复位的情况下，在一定的时间间隔之后，此时如果连接用户还没有提供登录的用户名及密码，Telnet 的对话将会超时。直到用户输入一个字符之后连接才会被复位。如果恶意用户连接到 Windows2000 的 Telnet 守护进程中，并且对该连接不进行复位的话，他就可以有效地拒绝其他的任何用户连接该 Telnet 服务器，主要是因为此时 Telnet 的客

户连接数的最大值是 1。在此期间任何其他试图连接该 Telnet 服务器的用户都将会收到如下错误信息：

Microsoft Windows Workstation allows only 1 Telnet Client LicenseServer has closed connection

察看“列出当前用户”选项时并不会显示超时的会话，因为该会话还没有成功地通过认证。

IIS 服务泄漏文件内容

这是一个 NSFOCUS 安全小组发现的漏洞。当微软 IIS 4.0/5.0(远东地区版本)在处理包含有不完整的双字节编码字符的 HTTP 命令请求时，会导致 WEB 目录下的文件内容被泄漏给远程攻击者。

Microsoft IIS 远东地区版本包括中文(简体/繁体), 日文，韩文版，由于特定的文字格式使它们都是使用的双字节编码格式。而当 IIS 接收到用户提交的一个 HTTP 请求时，如果文件名中包含非 ASCII 字符，IIS 会检查这个字符是否为双字节编码中的前导字符(例如，日文的前导字符包含两段字符：0x81-0x9F, 0xE0-0xFC)。如果是前导字符，它会继续检查下一个字符是否为结尾字符。如果没有下一个字符，IIS 会简单地丢弃这个前导字符，因为它并没有构成一个完整的双字节编码。然而，这种处理将导致 IIS 打开不同的文件而不是用户在请求中指定的文件。

攻击者通过提交一个特殊格式的 URL, 可以使 IIS 使用某个 ISAPI 动态链接库打开某种它所不能解释的类型的文件，并获得该文件的内容。依赖于系统安装的 ISAPI 应用程序的类型，攻击者可能获得 WEB 根目录或者虚拟目录下的文件内容，这些文件可以是普通文本文件(.asp, .ini, .asa 等等)，也可以是二进制文件(.exe 等

等)。

黑客们会使用 Unicode 的方法利用这个漏洞：

Unicode（统一的字符编码标准，采用双字节对字符进行编码）可以说是近一段时期以来最为流行的攻击入侵手段，仅国内近期就有江民公司等几个大的网站被这种入侵手段攻击。那我们就来谈一下这个很容易的利用 Unicode 漏洞配合 IIS 的漏洞进行入侵吧。

上面我们提到过由于某些双字节的 Windows2000 在处理某些特殊字符时与英文版本不同，然而利用这种 IIS 的漏洞，攻击者就可以通过这些特殊字符绕过 IIS 的目录审计远程执行任意命令。

http://server/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

黑客们其实只要下面两句很简单的指令绕过 IIS 的审计就能够对网站的页面进行改写，所谓的黑了一个网站就是这么的简单。

http://server/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+d:\inetpub\scripts\123.exe

http://server/scripts/123.exe?/c+echo+黑掉啦?+>+c:\inetpub\wwwroot\default.asp

这个问题已经在 IIS 4.0 + SP6 中得到解决，然而微软却让它在 IIS 5.0 中再度出现。

但该漏洞不会影响包括英语版在内的其他语言版本的 IIS 4.0/5.0。

MS SQL Server 的 SA 空密码攻击

在 Windows2000 中，企业级的用户一般都会用到另一个微软的产品，这个产品就是数据库管理软件 MS S

QL Server，但是在与 MS SQL Server 配合使用中，我们发现了很多的问题。最后我们就简单讲一下安装了 MS SQL Server 的 Windows2000 的网络操作系统普遍面临的安全问题。

在安装 MS SQL Server 后，MS SQL Server 会将产生一个默认的 SA 用户，而且初始密码在管理员没有设置的情况下为空。但是 SA 是 SQL Server 中非常重要的安全模块成员，这样一来黑客们就可以通过 SQL Server 的客户端进行数据库远程连接，然后再通过 SQL 的远程数据库管理命令 xp_cmdshell stored procedure(扩展存储过程)来进行命令操作:

xp_cmdshell "net user id password /add"

Xp_cmdshell "net localgroup Administrators id /add"

就以上两条简单的命令入侵者就能在 MS SQL Server 的服务器上马上新建一个管理员级别的 Administrators 组的用户。所以我们这里提醒各位网管大人，在安装好 SQL Server 您需要做的第一件事就是把 SA 的空密码立即进行修改。这个问题就不要我告诉你应该在哪里改了吧?

而且在一般情况下，一些功能对管理员来说也是没有必要的。如果你不需要 MS SQL Server 的 xp_cmdshell(use sp_dropextendedproc "xp_cmdshell")这项功能就不要把 xp_cmdshell extended stored proc(扩展存储过程)命令功能留着。

我们只需要在 isql 窗口中输入：

use master

sp_dropextendedproc 'xp_cmdshell'

然后打上 Service Pack 3，这里提醒管理员们一下，一定要经常留意微软的补丁包文件，并且注意及时的把系统和软件更新到最新的补丁。

本文中我们讲述了几个近期来最为流行的漏洞和攻击方法，他们实现入侵是如此的方便，这里可有不少的网友会认为 Windows2000 是一个不安全的操作系统，但如果你这样的认为那就说明我的文章还没有写明白，所以在最后我要强调一下，只要我们常打补丁包，正确的给系统加设密码，我们的安全率就在 85%左右。

如何使 Web 更安全

在某种程度上我们可以说，没有 Web，就没有 Internet。可是在大部分情况下，Web 应用程序及 Web 站点往往易遭受到各种各样的攻击，Web 数据在网络传输过程中也很容易被窃取或盗用。因此如何能够使 Web 及数据传输更加安全，是一个应该引起广泛注意地问题。

从总体情况来看，保护 Web 站点免受攻击的最重要的措施就是加强安全意识和提高安全防范措施。

一般情况下，攻击者攻击 Web 的主要目的在于：

1、非法偷窥；

2、伪装成 Web 站点的合法访问者；

3、伪装成 Web 站点管理员；

4、试图控制 Web 站点主机。

一、 非法偷窥

阻止 Web 攻击者监听行为的最有效方法就是要对 Web 站点和访问者之间所建立的连接进行有效加密。几

乎所有的 Web **浏览器和服务器都具备发送和接收加密通道上的数据的能力，这些加密数据被** SSL **和** TLS **这两个相关的协议管理。其中** SSL **由** Netscape **产生，**TLS **与** SSL3.0 **兼容。图** 1 **是微软公司的** IE5.0 **浏览器软件中的** Internet **选项，它显示了有关安全问题的协议。**

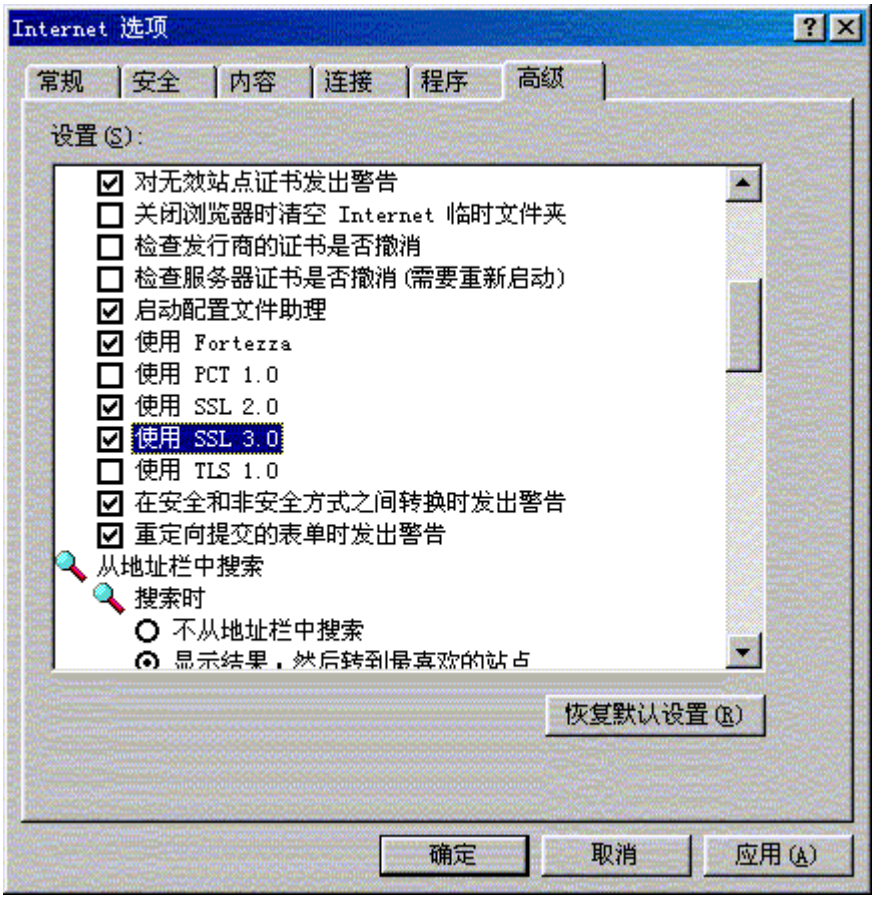


图 1IE5.0 **支持的各种加密协议**

Web **浏览器在连接一般的** WEB **站点通常使用的是** HTTP**（超文本传输协议），地址栏中** URL **一般形式为** http://www.somewhere.com**。而当** Web **浏览器连接到一个安全站点时，浏览器将使用** HTTPS **（超文本安全传输协**

议)来建立一个加密连接，地址栏中的 URL 通常的形式为 https://www.somewhere.com。

为了建立一个安全连接，Web 浏览器需要首先向 Web 服务器请求数字证书，数字证书提供了身份证明。浏览器在向 Web 服务器请求它的数字证书时，也同时发送了它所支持的加密算法列表。当服务器回送数字证书和它所选择的加密算法后，浏览器通过检查数字签名和确认 URL 是否与数字证明的公有名字域相匹配来验证数字证书。如过这些测试失败，浏览器将显示警告信息。如图 2 所示。

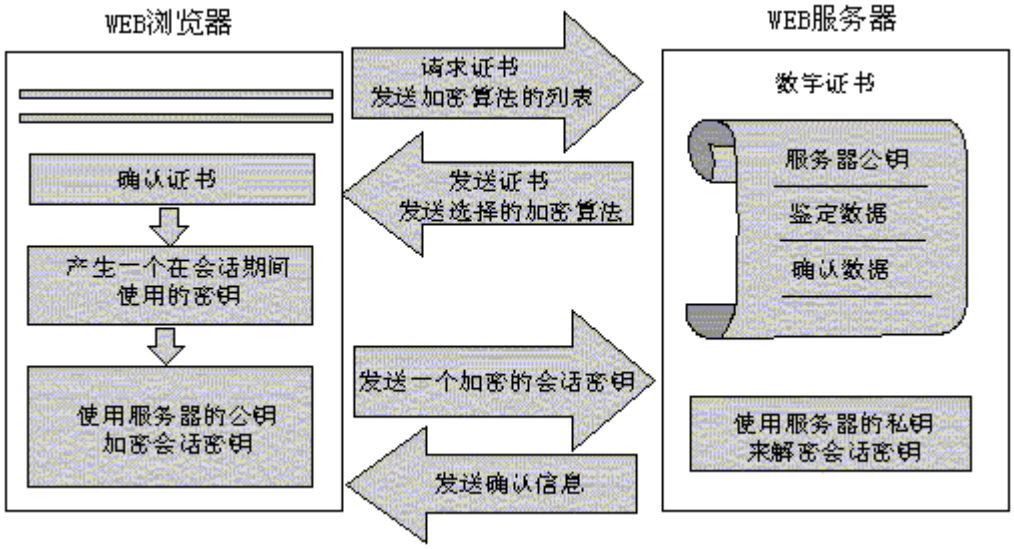


图 2Web 服务器对 HTTPS 的鉴定

浏览器和服务器的通讯使用对称加密。这就意味着使用相同的密钥来进行加密和解密。当服务器的证书被证实后，浏览器将产生一个密钥，这个密钥需要通过一个安全的途径传递给服务器。一般使用双重加密术来完

成密钥的传递。浏览器使用服务器的公钥来加密密钥，然后把它传递给服务器。服务器使用它的私钥来解密密钥然后向浏览器发送确认。

上面的过程表明的就是一个加密连接，浏览器和服务器都拥有相同的密钥，他们使用相同的加密算法。他们后面的通信将使用这个加密的连接。浏览器显示一个黄色的锁的图标表示连接已建立。如图 3 所示，站点访问者可以点击黄色的图标来检查服务器的证书，从而核实服务器的身份。

图 3 安全连接

建立一个加密连接，仅需要服务器获得权威机构（如 VeriSign）颁发的证书。但是加密仅能阻止攻击者看到站点发送和接收的数据，它并不能阻止攻击者伪造身份和对站点进行的恶意攻击。

二、伪装成 Web 站点的合法访问者

现在我们已经知道如何鉴别一个 Web 站点，但是一个站点如何鉴别它的访问者呢？下面我们就接着讨论这个问题。

大部分 Web 服务器支持两个密码鉴别方案：基本密码鉴别和分类密码鉴别。两个方案都通过向浏览器发送鉴别信号来进行。当浏览器第一次收到鉴别信号时，它显示一个对话框询问用户的名字和密码。在基本鉴别模式中，浏览器以简单的文本形式来传递用户名和密码。在分类鉴别模式中，浏览器传送用户名和密码的消息类。如果服务器发送它的证实，浏览器就把登录信息存储起来。

如果你用 Web 服务器上的简单设置来实现这些鉴定方案，Web 应用程序中不需要添加任何代码。

攻击者的监听问题：如果访问者以简单的文本形式发送他的用户名和密码，攻击者很容易就可捕获到这些信息。传送用户信息使用 SSL 可以很容易地解决这个问题。如下面的例子所示。

窗体顶部

User ID: < input type="text" name="user" >

Password: < input type="password" name="password">

窗体底部

如果攻击者不能监听 Web 站点和访问者之间的通信，他将要采取更加卑劣的手段——伪装成你的合法访问者。造成这种情况出现的原因一般是访问者自己造成的，因为大部分网络用户在密码选取上不是很留心，他们的密码一般都不是很安全。他们在登录各个站点时，喜欢使用相同的用户名和密码。

解决这个问题的方法就是访问者在注册帐号时要使用安全的密码。Web 站点最好具有能阻止访问者设置英文单词作为密码的功能，它可以建议用户使用数字和字母混合而成的密码。

三、伪装成 Web 站点管理员

当访问者登录到你的站点时，你将会保持他们的身份一直有效，直到他们离开该站点。那么如何实现这个功能呢？因为在浏览器和服务器之间不会建立一个永久的连接，所以服务器会在收到每个页面请求后只建立一个单独的连接。

用户登录成功后服务器是如何证实该用户的身份呢？

答案是浏览器保存了用户的姓名和密码。当浏览器和服务器再次连接时，浏览器将传递已经存储过的用户名和密码。服务器利用用户数据库来证实这些信息，并会在此基础上作出允许和拒绝访问的决定。

前面我们提到过，浏览器通过比较带有服务器的数字证书的公有名字的 URL 来证实服务器的身份。这是一个很好的 Web 安全防范措施。但是它不能避免所有的伪装服务器的攻击。

域名服务系统（DNS）可把易读的网址（例如 www.yourunit.com）解析为 IP 地址，在你的安全链接中它是一个易遭受攻击的链接。如果攻击者访问了一个 DNS 服务器，并且修改了指向他的机器的记录，那么这个机器就可以把所有来自 www.yourunit.com 站点的请求全部重定向到 www.attacker.com.。在重定向中，访问者的浏览器将显示默认的地址后缀。如果字符串很长，使 www.attacker.com 不在视野之内，大部分访问者都不会注意到。

如果攻击者得到 VeriSign 为 www.attacker.com 颁发的数字证书，那么访问者的浏览器将和 www.attacker.com 建立合法的连接。如果访问者不检查数字证书，他不会知道自己在一个黑客站点上。如果攻击者把他的站点伪装成为和 www.attacker.com 的登录界面一样的话，他就能捕获到该客户的银行信用卡帐号。

四、试图控制 Web 站点主机

一些攻击利用 web 服务器上运行的软件的漏洞来让服务器执行攻击者的代码。一类臭名昭著的攻击方法就是向缓存写入大量的数据从而使缓存器崩溃。下面所摘录的一段 C++代码就很容易受到这样的攻击，因为它没有边界检查。

```
void ByYourCommand( char* pszData )
{ char szBuffer[ 255];
strcpy( szBuffer, pszData ); ...}
```

如果执行 strcpy()过程使堆栈溢出，将会产生什么结果呢？图 4 向你展示了系统堆栈溢出后的情况。如果攻击者在缓存中写入了太多的数据，它将覆盖函数调用记录。这是一个数据结构，它包含了保存函数入口代码的

寄存器，还有函数的返回地址。如果攻击者的代码覆盖了函数的返回地址，攻击者就可以在你的计算机上执行任何代码。

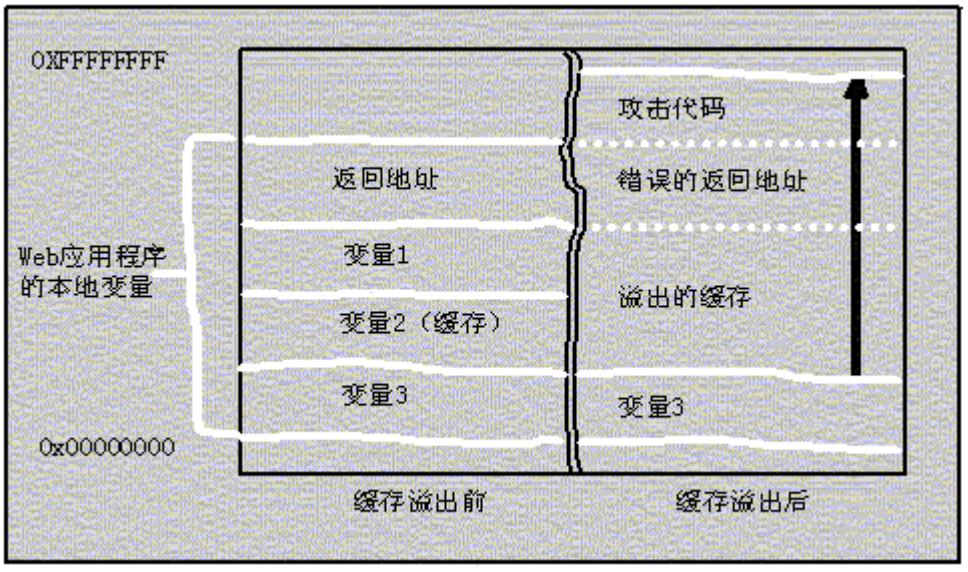


图 4 通过使缓存溢出，攻击者把攻击代码加载到内存，代替函数的返回地址，从而执行攻击代码

攻击者是如何把他的攻击代码移植到你的电脑上的呢？他使用的方法就是把代码写进数据缓存，传递这个例子函数的字符串很容易感染上“特洛伊木马”这样的黑客程序。有许多文章已经介绍过这类的攻击方式。

黑客知道易攻击的函数(例如上面所举的函数例子)通常易被回应用户输入的代码所调用。攻击者发送一个不可能的长字符串给服务器。如果缓存溢出，处理他的请求的线程将崩溃。攻击者得到 HTTP 超时的消息提示

就表明请求线程已被破坏。

如何阻止你 Web 站点的应用程序被利用呢？首先，给系统软件添加最新的安全补丁。然后，检查使用允许直接访问内存的语言（例如：C、C++和 Delphi）编写的程序代码，看是否有安全漏洞。

检查代码可以给你无尽的信心，因为你可以发现一个应用程序并不是很容易就受到缓存溢出这样的攻击的。如果你要完全避免这样的问题，只能不使用直接访问内存的语言来编写代码。你可以使用一些脚本语言（例如：JavaScript、Perl）或使用解释性的语言（例如 Java）。如果使用安全的语言来编写代码，Web 站点的操作员就可以被解放出来，不用天天担心缓存溢出这样的安全攻击。

另外，你也不要盲目地相信各种安全技术，厂商虽然为了推销自己的产品而做出了很好的安全质量承诺，但是你要知道没有任何技术能够保证你的 Web 不遭受攻击。所以你需要一定的时间和精力去研究和发现 Web 的缺点，然后找出解决问题的方法。

Web 的安全性问题非常复杂，范围很广，在本文中，我们只是从外部的攻击角度出发，讨论了如何避免 Web 应用程序和 Web 数据遭到破坏和窃取，来防止非法用户对 Web 应用程序的越权访问，提高 Web 站点的安全性。

纵横捭阖反病毒软件

反病毒软件是如今的电脑用户必备的工具软件之一，个人用户的踊跃购买成就了反病毒软件市场的兴旺

发达，造就了大大小小数十个品牌。面对这众多的反病毒软件，您知道选购它们的原则吗？您知道您在使用反病毒软件中可能存在的几个误区吗？您知道中国反病毒软件市场现状吗？您知道这些软件的优点、缺点吗？您知道如何合理搭配使用反病毒软件吗？本篇将带您走进令人眼花缭乱的反病毒软件世界，为您解答以上问题。

一. 反病毒软件的选购原则

反病毒软件的发展很快，市场上能够买到的产品也非常多，我们在选购时不能人云亦云，盲目跟从，应该有自己的原则。

首先，反病毒软件的优劣，并不取决于厂家的广告宣传，而是需要通过权威机构使用科学公正的方法加以认证。因为当产品通过权威机构质量测试时，权威机构就允许这些产品在出版时印上自身的标志，以权威机构本身的名誉担保产品的质量。因此，我们在选择反病毒软件时，不仅仅要看它们是否持有我国公安部颁发的计算机安全产品销售许可证，也一定要考查它们是否通过国际安全权威机构（如 ICSA 和 Checkmark）和计算机产品主流软硬件平台生产厂商（如 Microsoft 和 Intel）的多方认证。由于国际安全权威机构具有世界上最全面的计算机病毒样本库，反病毒产品如果通过这些机构的认证，则说明其查杀病毒的能力是可信的；而通过权威软硬件平台的测试认证，则说明该产品与这些软硬件平台不存在任何兼容问题，并且不会影响软硬件平台的运行效率。当然，在此基础上，打探一下反病毒软件在用户中的口碑如何，对我们的选购也是一个比较有用的参考。

其次，反病毒软件作为计算机安全产品中的一种，

其可靠性、兼容性与它的反病毒效果同样重要。我们不能光注意反病毒软件宣传的杀毒数量和种类的多少，也要注意它们的可靠性、兼容性。试想一下，一个杀毒数量和种类都很多的软件经常与机子中其它软件发生冲突，导致死机现象频繁发生，这样的鸡肋软件对您又有什么用呢？实际上这一条是对第一点中软硬件平台测试认证的一个补充，此时考察的重点是反病毒软件在与其它常用软件同时使用时的可靠性和兼容性如何，这一点同样很重要。

第三，反病毒软件的实时监控功能很重要。由于技术的发展加上更为广泛的信息交流，病毒的传播早已不分国界。象 CIH 这样的病毒已经能够作到无孔不入，如果我们还停留在使用静态反病毒产品阶段，最终的结果必然是被动挨打、防不胜防。当代计算机病毒最明显的一个特点，就是已经能够将病毒的作用机理与操作系统底层技术紧密结合起来。比如 CIH 病毒使用了 Windows 95/98 特有的 VxD 技术，它仅仅感染 Windows 95/98 系统，但对 DOS 及 Windows NT 系统则没有任何影响。这种能够与操作系统紧密结合的病毒针对特定系统，不但传播隐蔽，而且速度很快，令使用传统反病毒手段的用户很难及时发现。使用带有实时监控功能的反病毒软件，就可以为计算机构筑起一道动态、实时的反病毒防线，拒病毒于计算机系统之外。

第四，反病毒软件对压缩文件检测能力的强弱和支持压缩文件格式的多少，可以成为我们选购的一个重要依据。Internet 和分布式计算的日益普及，使数据交换摆脱了传统物理介质（如软盘等）的束缚。一般从 Internet 下载的共享软件都是压缩文件包，Internet——特别是

在 Internet 上转输的压缩文件所携带的病毒，正在对我们的计算机系统构成严重的威胁，压缩文件已逐渐成为了计算机病毒传播的温床。因此反病毒软件具有压缩文件反病毒检测能力是非常必要的。同时我们也应看到 Internet 上流行的文件压缩标准有很多种，相互之间并不兼容。所以我们在选择具有压缩文件反病毒检测能力的产品时，一定要搞清楚它们是不是能够适用于所有流行、通用的压缩格式，否则相当于给我们的反病毒工作留下了一个死角。例如有些反病毒产品能够检测扩展名为 ZIP 之类的压缩文件，但不支持用户自定义的扩展名和诸如微软 CAB 这样软件生产商专用的压缩格式，这样的软件我们当然不能选购。

第五，在技术方面，反病毒软件除了要有实时监控功能和压缩文件反病毒检测功能外，还应具有如下一些技术：内存解毒技术、查解变体代码机和病毒制造机技术、虚拟机技术、未知病毒预测、实时解毒、病毒源跟踪、应急恢复、Vxd 和 VDD 技术、查解 Trojan、查解 Java 病毒、查解宏病毒、多平台支持、网络反病毒-……这些都是判断一个反病毒软件好坏的重要标志！同时也是判断一个反病毒软件技术是否先进的一个标志。作为普通用户您可能不知道这些，但您可通过各厂商的宣传资料比较而知，再有从其他用户和报刊媒体（如电脑报）中也能得知这些。

另外，反病毒软件的防病毒、检测病毒和消除病毒的能力是首要的。在此基础上，作为反病毒软件它的误报率不能太高，查毒速度应该较快。应急恢复功能是一个优秀的反病毒软件所必须具有的功能，它创建的急救盘必须包括本机的 DOS/WINDOWS 启动文件，能够正

确备份和恢复主引导记录和引导扇区，以便在系统受病毒侵犯而崩溃时进行恢复。版本智能升级功能同样很重要，在公安部的检测中它也占有一席之地。另外一个好的反病毒软件应有良好的用户界面和全面的在线帮助手册以及翔实的病毒资料，以方便使用和管理。反毒软件的安装和卸载均应以向导形式进行,并应提供多种选择，这样可以方便用户同时使用两种以上的软件，在某些功能上根据各软件的特点加以取舍，这虽然不是一定要有的，但通过它可以看到一个反病毒软件在微小细节上做得怎样。

最后要把售后服务质量作为考察重点对象。由于病毒的产生日新月异，每天都有新病毒产生，因此要求反病毒软件厂家提供及时、快捷、简便的升级服务。同时由于反病毒软件将在不同的计算机环境下被不同熟练程度的用户使用，这就要求反病毒软件厂家为不同用户提供不同的服务，诸如解答用户在安装、卸载、使用反病毒软件过程中遇到的问题以及对用户计算机异常现象的处理等。最后，反病毒软件升级速度的快慢也是我们要考察的重点，它显示了厂家对新病毒反应速度的快慢和对用户服务的及时性。如同医院一样，反病毒软件厂家应为用户提供有关病毒防治的全天候服务，并且要求及时、准确。服务态度的好坏也是我们考察的重点，谁让用户是上帝呢。

二. 国内几款反病毒软件点评

由于大家使用最多的是国产反病毒软件，再加上国产反病毒软件宣传做得很多，因此大家对其优点了解较多，但对其不足就知之不多了，所以有必要在优点、缺点都谈的基础上对其进行一番点评，让大家对国产反病

毒软件有更深刻、更清醒的认识。

KV3000 是江民公司的产品(图 1)。作为国内反病毒软件的老牌霸主，KV 系列创造了中国反病毒软件销售的奇迹，连续多年市场占用率第一。新产品 KV3000 和老产品 KV300+相比，在各个方面都有了较大的提高与改善：无论是人机界面、功能的设置还是查杀病毒种类等都有所改进。 KV3000 可以运行在更多的操作系统下：它支持 DOS、Windows 3.x、Windows 95/98、Windows Me、Windows NT、Windows 2000 等系统。KV3000 可以查杀更多的计算机病毒种类和数量；提供更加完善的硬盘救护箱功能，使得硬盘数据的恢复工作异常简单；新版本增加了多种查杀计算机病毒的方法，加入了功能更加强大的“虚拟机法”、“神经网络敏感系统”等查杀计算机病毒的最新技术；它可识别的压缩文件的格式更多了，新增了微软 CAB 文件格式、WWPACK 格式、LZH 格式，同时可以识别这些压缩文件生成的可执行文件；升级也更加方便、快捷；清除宏病毒的功能得到很大的提高；提供详细的检查病毒的报告文件；提供清除病毒向导功能；提供自动定时扫描功能。

点评：比起原来的 KV300 系列， 江民公司的 KV3000 有了质的飞跃，查杀毒数量和种类都增加了许多，支持各种邮件编码格式检测，对邮件病毒也能查杀。由于采用了最新技术使它的性能有了明显提升。它的问题是更新速度稍慢，对新病毒的反应也不够快，再有就是著名的“硬盘逻辑锁”事件也降低了它在用户心目中的地位。

瑞星 2001 是瑞星公司的产品(图 2)。作为国内反病毒软件市场占有率的新盟主，其实力不容小视。该公司

最新的产品瑞星 2001 采用新一代病毒扫描引擎（VST）技术，可全面处理 DOS、Windows 3x、Windows 9x、Windows Me、Windows NT、 Windows 2000 等各种操作系统平台上的病毒。包括宏病毒、互联网病毒、黑客程序、邮件病毒以及其他类型的各种病毒。采用先进的实时监控技术，不仅可对传统的文件系统进行保护，并且对电子邮件系统也可进行实时高效的防护。当用户在发送、接收和打开电子邮件时，瑞星杀毒软件将自动对邮件本身及附件进行监控，一旦发现病毒将自动进行清毒，确保用户的邮件无毒，彻底切断病毒的感染通道；病毒隔离系统将带毒文件隔离到安全区域，在需要的情况下安全恢复，完全避免了因设置或其他误操作引起的重要文件丢失。作为该公司的用户，您可以把备份的未知病毒发给瑞星公司，以进行具体的病毒分析；它还提供智能升级功能，采用增量方式，无需访问瑞星主页，不必下载庞大的程序包，只需轻轻一点鼠标，即可自动升级。独有的断点续传工具则大大地提高了智能升级的效率；它还支持 DOS、Windows、Unix 等系统的几十种压缩格式，如 ZIP，GZIP，ARJ，CAB，RAR，ZOO，ARC 等，使得病毒无处藏身。

点评：与以往的版本相比，瑞星 2001 的兼容性有所提高。瑞星对新近出现的流行病毒的查杀效果很明显，其网络版在公安部组织的评比中获得了第一名的佳绩。但由于它是基于 235K 的病毒库，所以查杀毒数量始终是瑞星的瓶颈。

KILL2000 是冠群金辰的产品(图3)。它综合运用多种先进的查毒技术，可以彻底查杀宏病毒、传染 Windows 95/98 的病毒、Windows NT 病毒等国内外各种病毒甚至黑客工具，并能防止部分未知病毒对系统造成危害。 KILL2000 独有主动内核（Active K）技术，将多种反病毒技术嵌入操作系统和网络系统内核中，改传统的被动杀毒为主动防毒；它为用户提供了全面的 Internet 和网络病毒实时防护和治愈功能，包括黑客程序及可执行文件、压缩文件、电子邮件、Office 文档、HTML 文档等多种文件类型的监测。KILL2000 集预防、检测、清除、治愈自动化为一体，形成了立体全方位的自动化实时反病毒机制；和同类产品相比 KILL2000 系统资源占用率较低，用户还可以根据实际使用情况调配系统资源占有率，确保查杀病毒过程不会影响用户系统的使用；完善的服务体系除了提供传统的售前咨询、售后技术支持及热线服务外，还主动将最新升级文件和病毒消息发送到用户手里。此外，冠群金辰在全国有 50 多家授权服务中心，能给用户提供满意的服务。

点评：冠群金辰的 KILL2000 是唯一通过 ICSA 认证的国产反病毒软件，它在技术层面上不输于国内任何一家对手。由于采用了独有的反病毒技术—主动内核（ActiveK），会“主动”从操作系统的内核与应用环境无缝

连接，因此形成了立体式反病毒机制。此外，KILL2000 还拥有预定扫描、借助 Internet 的病毒特征码自动更新、多种病毒处理方式、病毒日志、灾难恢复等多种特性。借助公安部在国内建立的多个病毒检测网和 CA 公司（世界第二大软件公司）在 40 多个国家、170 多个城市建立的世界最大的国际病毒检测网，冠群金辰对新病毒的快速反应能力很突出。KILL2000 在快速扫描模式下，可检测后门程序数量过少，再有它的查毒速度较慢。我认为 KILL2000 若能在防范黑客程序方面能够进一步加强就极有可能成为中国 Anti-Virus 业的顶尖级产品。

金山毒霸是金山公司的产品(图 4)。在正式版上市前进行了大规模的测试活动，取得了不错的评价。金山毒霸采用了独特的双杀毒引擎，它由金山自主开发的杀毒引擎和俄罗斯科学院计算中心开发的 DrWeb 反病毒软件的杀毒引擎组成，一套软件相当于两套软件的杀毒功效，查毒病毒的范围更广，通过双引擎双重查杀，准确性更高；金山毒霸可查杀两万多种病毒家族和近百种黑客程序，除传统的病毒外，还能查杀最新的 Access、PowerPoint、Word 2000、Java、HTML、VBScript 等病毒，具备完善的实时监控(病毒防火墙)功能，支持 ZIP, RAR,CAB,ARJ 等多种压缩格式，支持 e-mail、网络查毒，具有功能强大的定时自动查杀功能；金山毒霸采用了最新的启发式搜索技术,通过对可疑文件特征的分析，能够确认是否是病毒,由于金山毒霸的双引擎双重判断，使防范未知病毒的准确性大大提高，误报率下降；它的增量升级也很有特色,每次只下载十几 K 或几百 K 大小的病毒库的增加部分，自动完成更新。

点评：金山毒霸采用了独特的 DoubleEngine 双杀毒

引擎，双重查杀，对病毒可以进行筛网式的搜索，增强了用户系统的安全性。金山毒霸在查杀黑客程序方面有其独到的一面，是国产反病毒软件中做得比较好的。它的问题是目前查杀病毒数量和种类不是特别多，不过它升级更新速度很快，平均每１时即新增查杀１种病毒。另外我们在使用中发现在查杀大的压缩文件时金山毒霸可能引起假死现象 !希望金山能加以改进解决这些问题。

VRV2001 是北信源公司的产品(图5)。它支持 Windows 95/98、Windows Me、Windows NT 、Windows 2000 等操作平台。能自动探测操作系统，智能选择安装版本。VxD、FSDs、FileHOOK、和 SYS 深层次与 Windows 系统衔接，稳定可靠。采用了多任务、多线程编程，合理调度系统资源，同时使用了任务间隙等优化算法，使 VRV2001 对系统资源占用率极低。VRV2001 版对目前流行的 Windows 平台都具有实时病毒防护功能。VRV2001 版能做到定位查毒，采用安全队列技术，并有启发式查毒功能，采用优化查毒引擎，能查已知数万种病毒，包括引导型病毒、文件病毒、蠕虫、邮件病毒、黑客程序、有害程序或恶意 JAVA 代码等。采用毒前杀毒技术，无论拷贝带毒文件，访问网络带毒文件，打开带毒文件夹，下载文件带毒，或打开邮件附件，防火墙都能立刻探测到，并可立刻清除。

点评：北信源的这款产品，界面不错，升级速度也很快，占用系统资源更少，查杀毒数量和种类也有大幅上升。特别是它在查杀有害程序或恶意的 Java Applets 和 ActiveX 控件等方面也有了很大进步（它以前的产品在这方面的表现不尽人意）。VRV2001 查杀毒速度很快，这使得它的漏查率高了点，检测多重压缩文件病毒的能力也有待进一步提高，同时它在查杀黑客程序方面，也有很大的改进空间。它的价格是这几款国产反病毒软件中最便宜的。

AV95III 是豫能信息技术有限公司在千禧之年推出的第三代反病毒产品(图 6)，它是 AV95 反病毒软件的一次重大改版和升级，包含了目前国际反病毒领域中的最新、最先进的技术和观念，全面集成数据安全、操作系统安全、Internet 网络安全软件的功能。其可查、杀的病毒种类提高到 24000 种以上,使用了内置“病毒防火墙”功能，可以保证绝对可靠的“在线式查杀”。内建第三代“病毒行为描述”、“虚拟机”、“启发式代码分析”等技术，可查杀各类变种、变形病毒和因特网蠕虫、黑客后门程序,支持在线邮件扫描。同时 AV95III是国内首个提出“可更换式引擎”概念的反病毒软件，可以实现核心代码级的扩充；也是国内软件行业中，首次在“核心引擎”级实现 PlugIns(插件) 技术的软件，用户升级只需要下载这些新模块(.DLL)。这使得在 AV95III中实现快速网络升级成为可能。

点评：AV95III 拥有令人眩目的个性化界面，它的加载速度快，升级速度也很快，高于每秒 4M 字节的超高速病毒扫描速度更快。虚拟机技术与广义病毒行为描述语言结合运用，使 AV95III在杀毒方面更准确、安全，

错杀、漏杀和遗留病毒僵尸等现象大为减少。它的不足是支持的压缩文件格式不多，查杀毒数量有待提高，实时监控功能也不够敏感，查杀黑客程序的表现也不令人满意。

安全之星是上海创源公司的产品(图 7)。查杀病毒超过 4 万种，采用基于 Win9x,Windows Me,Windows2000 底层设备驱动技术进行实时监控，与 Microsoft 操作系统无缝结合增加系统的稳定性；采用 VirtualRun 技术，准确查杀各类已知及未知病毒；专有的 MacroFinger 技术，基于 OLE，BIFF 格式精确查杀宏病毒；SafeMon 技术监视系统注册表跟踪异常操作及访问；安全之星同时具有网络防火墙功能，可查杀 BO（Back Orifice）、NetBus、NetSpy、Backdoor、冰河及 YAI 等 1000 多种黑客程序，个人防火墙开启后，当发现黑客攻击时进行报警并且阻止黑客的攻击。它可对 Internet 上目前已知的 1000 多种端口扫描及 DoS 攻击进行防御；它还具有升级提醒功能，真正一键升级，方便易用。

点评：安全之星的杀毒能力比较强，基本上它能查出来的病毒，它都能安全杀除，而不是通过改名或删除的方式。其最优秀之处就是做到了防火墙和病毒实时监控的完美结合，一个软件实现了病毒查杀+网络保护双重功能。在查杀黑客程序方面安全之星的表现是所有国

产反病毒软件中最好的。安全之星对交叉压缩文件的检测方面需要进一步增强。

三、国外几款主要反病毒软件简介

国外反病毒软件存在的主要问题是占用系统资源多，对国产病毒（尽管数量不多）查杀数量少，除了这两点外，国外优秀反病毒软件在技术上并不逊于甚至更胜国产反病毒软件一筹。目前它们还没有占据市场主流，选购国外品牌的用户并不多。基于以上两点事实使我们决定不对国外反病毒软件进行专门点评。

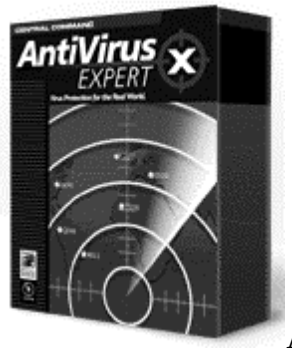
Norton AntiVirus 作为享有良好声誉的世界级品牌，大名鼎鼎的诺顿系列谁人不知、谁人不晓？！Norton AntiVirus (NAV) 特有的 Bloodhound 技术可以防止各种新型或变种病毒的侵害，启发式的扫描技术能够检测到类似病毒的活动，并可以在造成危害前及时消除未知病毒。它还可以有效的防止骇客以有破坏作用的 ActiveX 和 Java Applets 侵入您的计算机。Norton 对压缩文件的支持也非常不错，查病毒的速度也蛮快的，与操作系统的结合也很紧密。NAV 还可以保护个人资料的隐私权，并过滤网络广告网页，加速下载的时间。NAV 提供了最为出色的应急磁盘功能备份工具 Norton Rescue，它不仅支持生成急救软盘，也可用于 ZIP 盘进行更为完整的备份工作。NAV 的缺点是占用系统

资源多了一点，价格嘛也高了一些。您的机子若是性能不错，手头又不缺钱，一定不能错过这个软件。

McAfee 是反病毒软件世界第一品牌，世界排名前 100 家公司 80%用 McAfee。它采用了先进的双重智能扫描引擎，能及时发现新病毒、可疑病毒和未知病毒，所以，在病毒发作之前就可以有效地隔离感染文件；PSDE 引擎则高效查杀各种变形病毒；采用新一代扫描引擎 Virtran 定点扫描技术使扫描速度提高 70～90%。McAfee 查杀毒数量在 57000 种以上。McAfee 使用最新技术能够自动扫描网页，防止恶意的 Java Applets 和 ActiveX 控件，还可以自动检查从 Internet 下载的文件和电子邮件的附件是否含有病毒。国外的某些测评报告中，其检测与清除病毒的能力堪称最优。它能查杀的黑客程序是所有反病毒软件中最多的，当然，对付国产病毒和黑客程序它的表现就不敢称 NO.1 了。

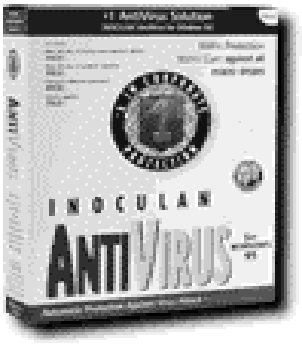
熊猫卫士是欧洲销量第一的品牌。它是世界上第一个能在 WINSOCK 层上进行病毒扫描的防病毒软件。基于 Winsock 层病毒防护极有特点，Winsock 是 Windows 和 Internet 的必经之路，因此基于 Winsock 层的病毒防护，就等于给您的计算机在 Windows 系统和 Internet 之间安装了病毒的过滤器，可以阻止任何来自于 Internet 的病毒。熊猫卫士铂金版集成了所有的 Internet 保护功能，具有智能、强大和便于使用的特点。它能对任何级

别嵌套的压缩文件进行快速扫描。熊猫卫士为 Internet 和消息系统提供了一个永久病毒防护模块，能对恶意的 ActiveX 控件及 Java Applets 进行有效防护，并且可对所有的 E-mail 程序进行完全防护。熊猫卫士铂金版还保持着一项世界纪录，同时拥有 ICSA 和 Checkmark 这两个权威安全认证组织的认证，它们授予熊猫卫士的证书比任何其它同类产品都要多，这是对它产品品质的最好印证和最高嘉奖。熊猫卫士的问题是查毒时占用系统资源比较多，机子性能差的用户最好不要试了。



AVP 是一套出色的俄罗斯防毒软件。大家可能对它不是很熟悉，但这个软件在国外可是好评如潮，褒奖不断。以前的 AV95 和 AV98 都曾大量采用了 AVP 的技术。俄罗斯出的软件不多，但似乎各个都是精品，AVP 亦如此。它没有其他软件那样大，比较节省硬盘空间。但该有的功能它都不缺，防毒功能更是不错，它也有常驻于 System Tray 的自动监视功能，可帮你自动监视从磁盘、网络上、E-mail 中打开文件的安全性。它也有鼠标右键的快速选单，还附有 LiveUpdate 线上更新病毒码的功能。早在去年 2 月份 AVP 就可查出冰河和黑洞 2001 等国产木马程序,可见它对国产黑客程序也不含糊。。目前 AVP 在中国没有注册点，最近的也在中国香港，当然您可以在它的主页找到它的共享版

本免费试用。



Inoculan AntiVirus 6.0 是 CA 出品的一款优秀的反病毒软件，著名的国产反病毒软件 Kill 其实就是 Inoculan AntiVirus 5.0 的中文版。Inoculan AntiVirus 6.0 目前只有英文版，但该软件操作简便，易用性好，即便你的英文水平不是很高使用起来。它的实时监控功能强大，占用系统资源也不多，对于压缩文件的查杀也很出色，对于宏病毒的检测也令人信服。它还可以自动检查从 Internet 下载的文件和电子邮件的附件是否含有病毒。Inoculan AntiVirus 6.0 在防止恶意的 Java Applets 和 ActiveX 控件等方面做得很专业，在此，向所有有钱、没钱的电脑用户推荐这个软件，它真的很优秀。相信我，没错的。

PC-cillin2001 是总部设在美国的台湾反病毒软件，因此将它列在反病毒软件中最后一个介绍，它的实际表现却与它的出场顺序毫不相干。PC-c

illin2001 是一款很不错的反病毒软件，除了传统的引导型、文件型及宏病毒外，亦可主动侦测、清除通过互联网入侵的 java script、ActiveX applet 等恶意程序，可全面拦截电子邮件及附件夹带的病毒入侵。它同时还首创“宏病毒陷阱”Macro Trap 技术，利用基于规则的分析来判断和确定宏代码是否感染了病毒，这种方式有效地克服了常规特征码查毒技术的不足；它的另一项独创的 WebTrap 智慧型 Internet 病毒陷阱技术，进一步加强了对系统的保护。PC-cillin2001 对压缩文件中的病毒查杀能力特别强，可穿透 20 层以上的压缩文件，支持 19 种以上压缩格式和 4 种解码格式，同时它的扫描速度很快。PC-cillin2001 在查杀毒数量方面有待进一步加强。

四、反病毒软件实用搭配方案几例

反病毒软件进行搭配的原则是实现功能互补和优势互补，并且相互间不能产生冲突，搭配后的可靠性、兼容性要有保证，搭配的结果应该是１＋１>2。在具体操作上，应是国外反病毒软件和国内反病毒软件搭配；资源占用率高的和资源占用率低的搭配；查杀病毒能力强的和查杀黑客程序能力强的搭配；单机防毒强的和网络防毒能力强的搭配。通过搭配组合，不但可以扬长（发挥自己的优势），而且可以避短（发挥对方的优势），同时还可以交叉查杀病毒，极大的增强了系统的安全系数。下面向您推荐以下搭配方案：

1、Norton AntiVirus 2001＋KILL2000

Norton AntiVirus 2001 查杀病毒数量极多，尤其值得称道的是 NAV 对捆绑了木马程序的软件识别率极高，国产反病毒软件难以望其项背。在木马程序泛滥成灾、

捆绑软件功能越来越强大的今天，安装 NAV 不失为一个明智的选择。KILL 长期以来一直是国产杀毒软件中做得非常出色的一个。KILL2000 与系统的兼容性很好，并通过了微软等公司的认证。KILL2000 还能够根据系统底层代码的不同进行分析，深入系统内部核心，使其实时监控具备高可靠性和高稳定性。在使用 KILL2000 时，漏报、误报、死机等现象很少发生。事实上，在随系统开启 Norton AntiVirus 2001 实时监控的情况下，病毒入侵这一组合的可能性已经非常小了。经测试，这个组合非常理想，在使用中未发现任何冲突现象。向机子性能不错的朋友强烈推荐这套方案。

2、熊猫卫士铂金版＋KILL2000

熊猫卫士铂金版无论功能还是操作界面都无可挑剔，对付国外病毒有优秀的表现，绝对是一个五星级的专业产品；KILL2000 功能强大，占用系统资源少，对付国产病毒表现也很不错。两个共同经过 ICSA 认证的反病毒软件搭配正是天作之合，给人以极强的信心，相信这也是大家梦寐以求的强强组合。这套搭配组合除了查杀毒数量及种类较多外，对恶意的 Java 应用程序和 ActiveX 控件监控表现也非常出色。它们之间的组合没有产生过冲突，与其它软件的兼容性也不错。这套搭配方案适用于大多数用户，如果您的机子是时下流行配置向您推荐这套组合。这套方案推荐给机子性能属于中高档的用户。

3、McAfee5.13＋瑞星 2001

McAfee 集成了所有的 Internet 保护功能，具有智能、强大和便于使用的特点。它能对任何级别嵌套的压缩文件进行快速扫描。在查杀毒数量和种类、宏病毒的侦测

及 E－mail 监控、恶意 Java Applets 和 ActiveX 控件实时监控以及黑客程序查杀等方面也有巨大的优势；瑞星 2001 则对国内流行病毒较为敏感，对国产病毒查杀率较高，占用系统资源也不多，同时查杀毒速度较快，再有瑞星的服务也非常到位，查杀不了的病毒在必要时可以请他们出面来解决。作为最新的国内外市场占有率各排第一的强强组合，这样一对搭配应该说是非常理想的，它们的实际表现也真的很不错。这套搭配方案适用于大多数用户，如果您的机子是时下流行配置向您推荐这套组合。

4、AVP＋金山毒霸

AVP 可以查杀包括变形病毒、针对 Windows 系统的 32 位病毒以及 Word 和 Excel 中的宏病毒。它拥有一个强大的启发式“ 代码分析器 ”，能够正确检测出所有已知病毒和 80%左右的未知病毒。对于压缩文件中的病毒，AVP 也能使用自己的解压缩引擎轻松对待。它还具有自我免疫功能，即使本身被病毒感染了也能够自动修复，保持自身纯洁。AVP 的实时监控功能称作 AVP Monitor ，对恶意的 ActiveX 控件 及 Java Applets 防护做得也不错，并且可对所有的 E-mail 程序进行完全防护。金山在办公软件和游戏软件这两方面取得了不错的业绩，进军反病毒软件市场后进行了大规模的测试，应该说产品质量还是有保证的。采用双引擎的金山毒霸在对付国产病毒和黑客程序方面很有一套，再加上金山强大的研发能力和完善的售后服务，使我们对金山毒霸很有信心，事实上它的表现也的确不错。在与 AVP 搭配后，整个系统运行稳定，无冲突现象发生，对病毒的反应及查杀都做得不错,占用系统资源也不多。这套方案推荐机

子性能不大好的用户使用。

5、PC-cillin2001＋KV3000

PC-cillin2001 对以网络为载体的病毒防治很有一套，对恶意的 Java Applets 和 ActiveX 控件监测做得也不错，对宏病毒的查杀更有不俗表现，在对黑客程序的监测方面也表现出了一定的水准，再有它对压缩文件的优良查杀能力也是我们选择它的一个重要理由，可以说是病黑程序双防，广普抗菌；而 KV3000 拥有很好的 DOS 性能和优秀的查杀国产病毒的能力是我门选择它的最大理由，它使得我们的电脑一旦中了病毒，还拥有在 DOS 下与其再战一场的本钱。KVW3000 还拥有庞大的病毒库，新增的神经网络敏感系统、虚拟查毒法、智能广谱法等查杀病毒手段也让我对它的信心大增。建议使用 PC-cillin2001 的实时监控程序。这对组合经过长期使用，未发现与系统或其他软件冲突。无论您的机子性能如何用这套方案都可以应付（PII 以下就免了吧）。

6、Inoculan AntiVirus 6.0+安全之星

作为世界第二大软件厂商 CA 公司的产品，Inoculan AntiVirus 6.0 本身就是品质的代名词，看看 KILL 的表现就应该知道 Inoculan AntiVirus 6.0 如何了。它查杀毒的数量即便是在国外反病毒软件中也是名列前茅的，再有它占用系统资源不多也是我选择它的一个原因，要知道对于一个国外反病毒软件做到这一点的实在不多；安全之星杀毒能力出色，可以几乎百分之百杀除它已知的病毒,同时它优秀的网络防火墙功能也使人爱不释手，在以上所有提到的反病毒软件中，安全之星查杀国产黑客程序的表现是最好的。在我们与网络联系愈发紧密的今天，这个出色的网络防火墙可以使我们的安全感大大

增强。这对组合在使用中未发生与其他软件兼容性方面的问题，相互配合也不错，功能做到了互补，占用系统资源非常少，是个不错的方案。推荐经济不大宽裕或机子性能不是很好的朋友使用。

以上搭配方案在查杀病毒时的表现很好，但也存在一个问题，那就是查杀黑客程序的能力有限（McAfee、NAV、安全之星在这方面表现虽然不错，但仍很不足），尽管已经做了尽可能的优化搭配，但限于反病毒软件本身查杀黑客程序能力的低下，导致这些方案在对付黑客程序方面有些力不从心，因此在实际使用中您要另外选择一款专门的防杀黑客软件搭配，当然您若不上网就另当别论了。在此，我们希望反病毒软件能够加强对黑客程序的查杀能力,毕竟网络时代黑客程序已无处不在了，增强黑客程序查杀能力也是大势所趋，人心所向。

以上有关反病毒软件的言论只是一家之言，在您选购和使用时可作为参考。由于每台电脑的性能及用途不同，大家对反病毒软件的喜好、认同点也不尽相同，因此对文章中提到的一些问题您可能会有不同的看法和做法，欢迎大家就这些问题与我探讨，共同进步。

浅谈网络的攻击检测技术

保证信息系统安全的经典手段是“ 存取控制 ”或“ 访问控制 ”, 但无论在理论上还是在实践中，这种手段都不能彻底填补一个系统的安全漏洞，也还没有一种切实可行的办法解决合法用户在通过“ 身份鉴别 ” 或 “ 身份认证 ”后滥用特权的问题。攻击检测技术就像治安巡逻队，

专门注重于发现形迹可疑者。

计算机网络技术的发展和应用对人类生活方式的影响越来越大。通过 Internet 网连接到几乎世界上任何一台计算机。因此，传统的安全域的概念也已经发生了深刻的变化，边界变得模糊了，网络系统管理员再也不能满足于守住安全边界了；也不再有信心保护敏感信息万无一失。越来越多的证据表明计算机信息系统的安全性是十分脆弱的。基于计算机、网络的信息系统的安全问题已经成为非常严重的问题。

一、存取控制与攻击检测：站岗与巡逻

保证信息系统安全的经典手段是“ 存取控制 ”或“ 访问控制 ”,这种手段在经典的以及现代的安全理论中都是实行系统安全策略的最重要的手段。但迄今为止，软件工程技术还没有达到 A2 级所要求的形式生成或证明一个系统的安全体系的程度，所以不可能百分之百地保证任何一个系统（尤其是底层系统）中不存在安全漏洞。而且，无论在理论上还是在实践中，试图彻底填补一个系统的安全漏洞都是不可能的，也还没有一种切实可行的办法解决合法用户在通过“ 身份鉴别 ”或“ 身份认证 ”后滥用特权的问题。打个比方，经典的安全体系就像一座城池，身份认证就好像进城时的查路条一样，着重点在于防范奸细混入；但是这种措施对于城池的安全仍是远远不够的。

攻击检测作为其他经典手段的补充和加强，是任何一个安全系统中不可或缺的最后一道防线；攻击检测可以分为被动、非在线地发现和实时、在线地发现计算机网络系统中的攻击者两种方法。从大量非法入侵或计算机盗窃案例可以清晰地看到，计算机系统的最基本防线

“存取控制”或“访问控制”，在许多场合不是防止外界非法入侵和防止内部用户攻击的绝对无懈可击的屏障。大量攻击成功的案例是由于系统内部人员不恰当地或恶意地滥用特权而导致的。攻击检测技术则类似于治安巡逻队，专门注重于发现形迹可疑者，信息系统的攻击者很有可能通过了城门的身份检查，或者爬越了城墙而混入城中；这时要想进一步加强信息系统的安全强度，就需要增派一支巡逻队，专门负责检查在城市中鬼鬼祟祟行动可疑的人员。

攻击检测提供了一种机制，对合法用户而言能够在一定程度上使他们为其失误或非法行为负责，从而增强他们的责任感。对非法进入的攻击者而言则意味着增强了纠察力度，行使着公安局、检察院的职责。攻击检测具有最后防线性质的防范能力，或许是用来发现合法用户滥用特权的唯一方法，而且完善的攻击检测还能用具有法律效力的方式证明一个受到怀疑的人是否有罪。

早期中大型的计算机系统中都收集审计信息来建立跟踪文件，这些审计跟踪的目的多是为了性能测试或计费，因此对攻击检测提供的有用信息比较少。

二、攻击检测技术

1．攻击分类

在信息系统中，一般至少应当考虑如下三类安全威胁：外部攻击、内部攻击和行为滥用。攻击者来自该计算机系统的外部时称作外部攻击；当攻击者就是那些有权使用计算机，但无权访问某些特定的数据、程序或资源的人企图越权使用系统资源时视为内部攻击，包括假冒者（即那些使用其他合法用户的身份和口令的人）、秘密使用者（即那些有意逃避审计机制和存取控制的人

员）;特权滥用者也是计算机系统资源的合法用户，表现为有意或无意地滥用他们的特权。

通过审计试图登录的失败记录可以发现外部攻击者的攻击企图；通过观察试图连接特定文件、程序和其他资源的失败记录可以发现内部攻击者的攻击企图，如可通过比较为每个用户单独建立的行为模型和特定的行为来检测发现假冒者；但要通过审计信息来发现那些权利滥用者往

往是很困难的。

基于审计信息的攻击检测特别难于防范具备较高优先特权的内部人员的攻击，因为攻击者可通过使用某些系统特权或调用比审计本身更低级的操作来逃避审计。对于那些具备系统特权的用户，需要审查所有关闭或暂停审计功能的操作，通过审查被审计的特殊用户、或者其他的审计参数来发现。审查更低级的功能，如审查系统服务或核心系统调用通常比较困难，通用的方法很难奏效，需要专用的工具和操作才能实现。总之，为了防范隐秘的内部攻击需要在技术手段以外确保管理手段行之有效，技术上则需要监视系统范围内的某些特定的指标（如 CPU、内存和磁盘的活动），并与通常情况下它们的历史记录进行比较，以期发现之。

2．攻击检测技术分类

基于计算机系统审计跟踪信息设计和实现的系统安全自动分析或检测工具是最为自然朴素的攻击检测技术。可以从审计系统筛选出涉及安全的信息。其思路与流行的数据挖掘（Data Mining）技术极其类似。

基于审计的自动分析检测工具可以是脱机的，也可以是联机或在线的。分析工具实时地对审计跟踪文件提

供的信息进行同步处理，当有可疑的入侵行为时，系统提供实时的警报，在攻击发生时就能提供攻击者的有关信息。

对于信息系统安全强度而言，联机或在线的攻击检测是比较理想的，能够在案发现场及时发现攻击行为，有利于及时采取对抗措施，使损失降低到最低限度。同时也为抓获攻击犯罪分子提供有力的证据。但是，联机的或在线的攻击检测系统所需要的系统资源，几乎随着系统内部活动数量的增长呈几何级数增长。

3．攻击检测方法

（1）基于审计的攻击检测

基于审计信息的攻击检测工具以及自动分析工具可以向系统安全管理员报告计算机系统活动的评估报告，通常是脱机的、滞后的。

对攻击的实时检测系统的工作原理是基于对用户历史行为的建模，以及在早期的证据或模型的基础之上。审计系统实时地检测用户对系统的使用情况，根据系统内部保持的用户行为的概率统计模型进行监测，当发现有可疑的用户行为发生时，保持跟踪并监测该用户的行为。

系统应具备处理自适应的用户参数的能力。能够判断使用行为的合法或可疑。系统应当能够避免“肃反扩大／缩小化”的问题。这种办法同样适用于检测程序的行为以及对数据资源（如文件或数据库）的存取行为。

（2）基于神经网络的攻击检测技术

如上所述，基于审计统计数据的攻击检测系统，具有一些天生的弱点,因为用户的行为可以是非常复杂的，所以想要准确匹配一个用户的历史行为和当前的行为是

相当困难的。错发的警报往往来自于对审计数据的统计算法所基于的不准确或不贴切的假设。SRI 的研究小组利用和发展神经网络技术来进行攻击检测。神经网络可能用于解决传统的统计分析技术所面临的以下几个问题：

●难于建立确切的统计分布

●难于实现方法的普适性

●算法实现比较昂贵

●系统臃肿难于剪裁

目前，神经网络技术提出了对基于传统统计技术的攻击检测方法的改进方向，但尚不十分成熟，所以传统的统计方法仍将继续发挥作用，也仍然能为发现用户的异常行为提供相当有参考价值的信息。

（3）基于专家系统的攻击检测技术

进行安全检测工作自动化的另外一个值得重视的研究方向就是基于专家系统的攻击检测技术，即根据安全专家对可疑行为的分析经验来形成一套推理规则，然后再在此基础之上构成相应的专家系统。由此专家系统自动进行对所涉及的攻击操作的分析工作。

所谓专家系统是基于一套由专家经验事先定义的规则的推理系统。例如，在数分钟之内某个用户连续进行登录，且失败超过三次就可以被认为是一种攻击行为。类似的规则在统计系统似乎也有，同时应当说明的是基于规则的专家系统或推理系统也有其局限性，因为作为这类系统的基础的推理规则一般都是根据已知的安全漏洞进行安排和策划的，而对系统的最危险的威胁则主要是来自未知的安全漏洞。实现一个基于规则的专家系统是一个知识工程问题，而且其功能应当能够随着经验的

积累而利用其自学习能力进行规则的扩充和修正。

（4）基于模型推理的攻击检测技术

攻击者在入侵一个系统时往往采用一定的行为程序，如猜测口令的程序，这种行为程序构成了某种具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图，尽管攻击者并不一定都是恶意的。用基于模型的推理方法人们能够为某些行为建立特定的模型，从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本，这种系统就能检测出非法的用户行为。一般为了准确判断，要为不同的入侵者和不同的系统建立特定的攻击脚本。

当有证据表明某种特定的攻击模型发生时，系统应当收集其他证据来证实或者否定攻击的真实，以尽可能的避免错报。

为了防止过多的不相干信息的干扰，用于安全目的的攻击检测系统在审计系统之外一般还配备适合系统安全策略的信息采集器或过滤器。同时，还应当充分利用来自其它信息源的信息。在某些系统内可以在不同的层次进行审计跟踪。如有些系统的安全机制中采用三级审计跟踪，包括审计操作系统核心调用行为的跟踪、审计用户和操作系统界面级行为的跟踪、和审计应用程序内部行为的跟踪。

总之，和经典安全措施相同，任何一种攻击检测措施都不能视之为一劳永逸的，必须配合有效的管理和组织措施，形成立体的和纵深有序的安全防御体系。

BlackICE：挡住黑客的魔爪

防火墙在最初的时期是建筑物中用来防止火势蔓延的一种防火设施，在计算机网络中这个概念也被引入了近来，但是计算机中的防火墙不在被作为防止火灾的设施，而成为了一种放置在网络内部连接点差距的设备和软件。

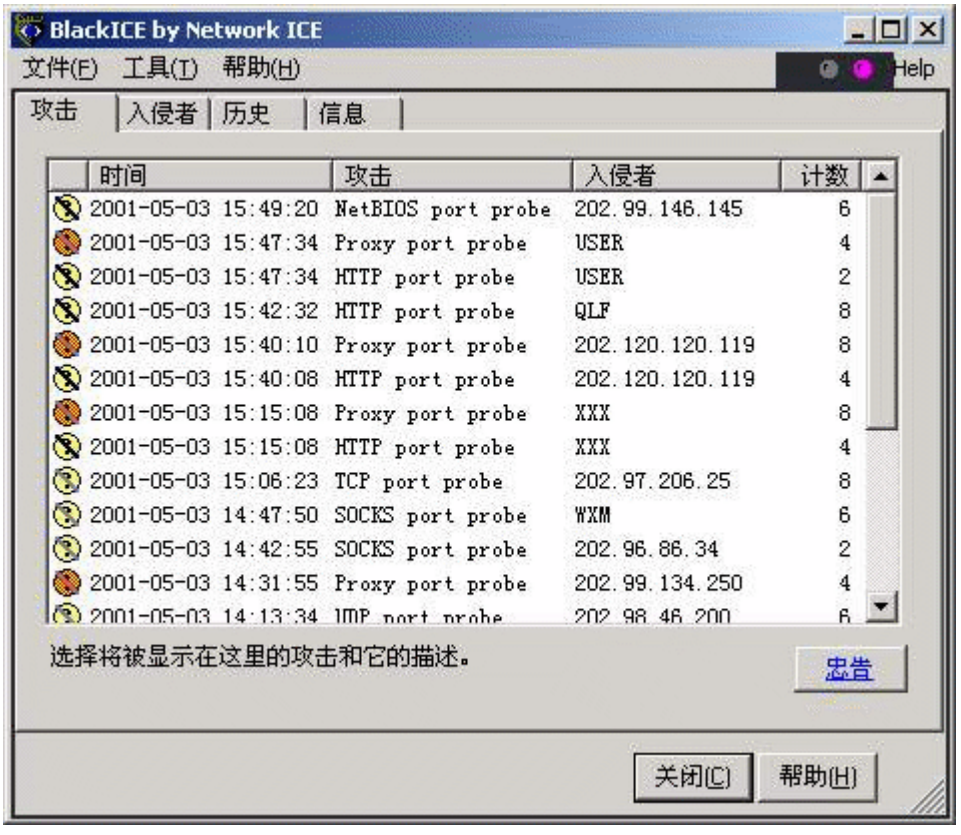
计算机在安装了防火墙后，任何的信息和数据在通过网络进行交换或者通讯的时候都会经过防火墙过滤和分析，而且多数防火墙系统在你的系统遭到攻击的时候还会发出警告。防火墙的工作方式很简单，它就是利用监控你计算机的端口与经过端口的数据来判断那些人是想攻击你的人，这个原理就好像我们出入超市时经过的磁性检测仪一样。

在众多的防火墙软件中笔者最为欣赏的是美国 Net WorkICE 公司的 BlackICE，BlackICE 是一款专门为 Windows9x/NT/2000 系统设计的防火墙软件，它具有相当强大的数据信息过滤系统，能过辨别几乎所有的计算机网络恶意攻击或者计算机网络中的恶意数据扫描。并根据攻击数据的危险程度作出不同的提示和警告，此外它还具有实时更新的功能，可以很方便地就在网上将防火墙的数据进行更新。

想要找到 BlackICE 很容易，国内很多大的下载网站都会有他的身影，当然你也可以在 http://download.yesky.com/servlet/mydown.yeskydown?tag=4&objID=584 进行下载。BlackICE 的最新版本为 2.5。

现在我就为大家介绍一下 BlackICE 的简单设置和使用方法，在进行完毕安装步骤后，我们很容易就会发现在我们的计算机屏幕的右下角出现了一个 BlackeICE 的小图标。

要想对 BlackICE 进行设置我们就要先双击这个小图标。首先我们看到的是一个攻击列表，这里是用来显示攻击你计算机的人的 IP 地址与攻击方法、次数和时间的列表。在下面的这个图二中我们可以看到大量攻击者的信息，其中有代理端口扫描攻击，HTTP 端口扫描，NetBIOS 共享扫描等等，而且在入侵者 IP 姓名后面还有入侵者的详细攻击次数。如果是在没有防火墙的计算机上面，计算机就会“无私”的将这些信息反馈给入侵者，或者是我们的计算机直接面临崩溃的与被入侵的危险。

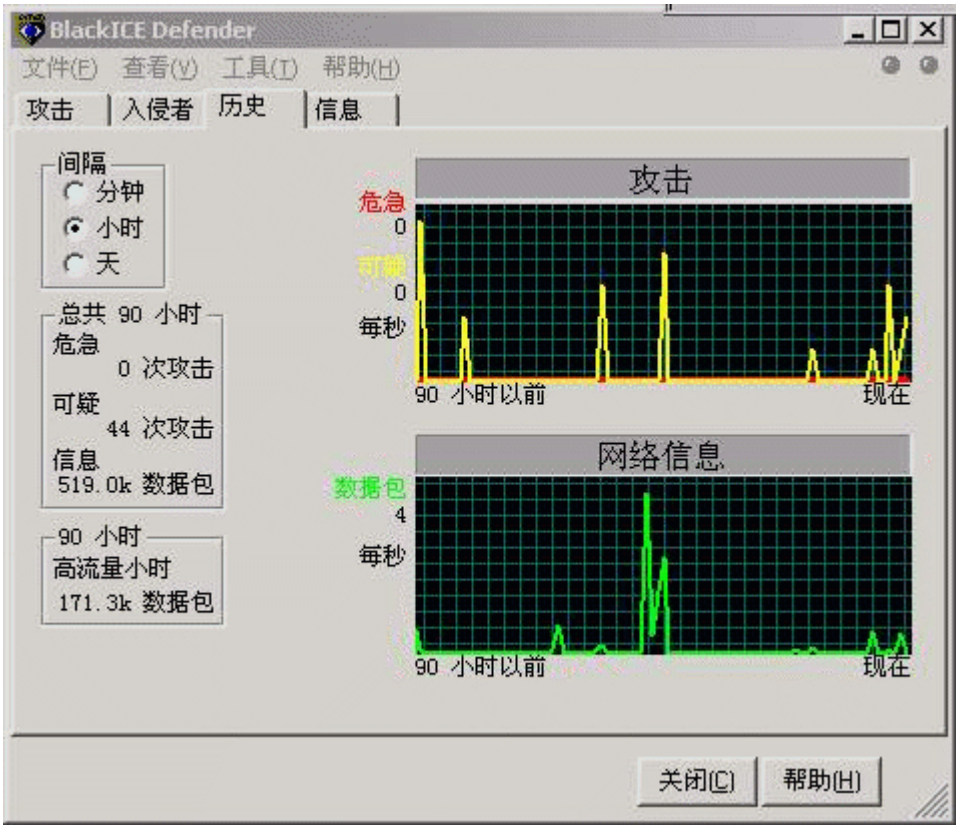


在列表的右下角还有一个可以点击的“忠告”按钮，这个按钮主要是用来让我们了解入侵者的攻击方法我们如何避免的一些措施的，看一看是很有帮助的。

知道了入侵者的 IP 并不是最重要的，ICE 还会根据情况来判断出入侵者的详细信息。我们点击攻击按钮后面的入侵者按钮，可以对入侵者的详细资料进行观察和分析。

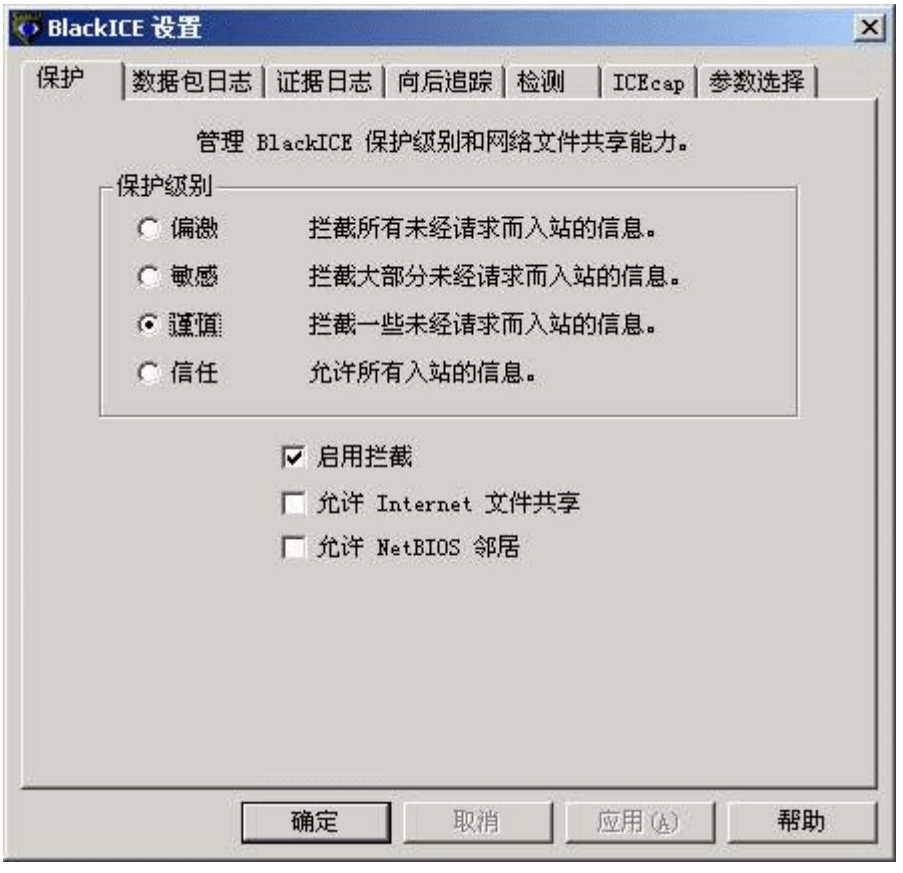
图中向我们揭示了入侵者的详细信息，其中包括入侵者计算机的姓名，入侵者的 IP 地址，而且根据上面的信息我们还刻有判断出入侵者使用的是 Windows ME 操作系统。这些信息对于我们了解入侵者和判断入侵目的都是很有帮助的。

而选项中历史的作用是让我们看到我们的计算机在不同的时段里遭到了那些攻击的高峰期，方便我们判断入侵者的习惯。



此外我们还可以根据自己的具体情况需要对 BlackICE **进行设置，我们点击工具按钮中的“编辑** BlackICE **设置”可以看到具体的设置选项。**

其中在保护一项我们可以设置防火墙的敏感度与拦截信息，另一个重要的参数选择，我们可以根据自己的习惯对防火墙的一些警告提示进行设置。


BlackICE 设置
保护
数据包日志
证据日志
向后追踪
检测
ICEcap
参数选择
管理 BlackICE 保护级别和网络文件共享能力。
保护级别
偏激
拦截所有未经请求而入站的信息。
敏感
拦截大部分未经请求而入站的信息。
谨慎
拦截一些未经请求而入站的信息。
信任
允许所有入站的信息。
启用拦截
允许 Internet 文件共享
允许 NetBIOS 邻居
确定
取消
应用(A)
帮助

通常的境况下我们不需要对设置进行改动，默认的设置就可以满足我们的需求。当我们计算机桌面右下角的小图标开始闪烁的时候，我们就可以根据这些情况分析出我们是否遭到攻击了。

当然最后我要说的是要及时经常的更新一下我们的防火墙啊。

系统被入侵后的恢复

准备工作

一、商讨安全策略

如果你的组织没有自己的安全策略，那么需要按照以下步骤建立自己的安全策略：

1.和管理人员协商

将入侵事故通知管理人员，可能在有的组织中很重要。在 be aware 进行事故恢复的时候，网络管理人员能够得到内部各部门的配合。也应该明白入侵可能引起传媒的注意。

2.和法律顾问协商

在开始你的恢复工作之前，你的组织需要决定是否进行法律调查。

注意 CERT(Computer Emergency Response Team)只提供技术方面的帮助和提高网络主机对安全事件的反应速度。它们不会提出法律方面的建议。所以，对于法律方面的问题建议你咨询自己的法律顾问。你的法律顾问能够告诉你入侵者应该承担的法律责任(民事的或者是刑事的)，以及有关的法律程序。

现在，是你决定如何处理这起事故的时候了，你可以加强自己系统的安全或者选择报警。

如果你想找出入侵者是谁，建议你与管理人员协商并咨询法律顾问，看看入侵者是否触犯了地方或者全国的法律。根据这些，你可以报案，看看警方是否愿意对此进行调查。

针对与入侵事件，你应该与管理人员和法律顾问讨论以下问题：

如果你要追踪入侵者或者跟踪网络连接，是否会触犯法律。

如果你的站点已经意识到入侵但是没有采取措施阻

止，要承担什么法律责任。

入侵者是否触犯了全国或者本地的法律。

是否需要进行调查。

是否应该报警。

3.报警

通常，如果你想进行任何类型的调查或者起诉入侵者，最好先跟管理人员和法律顾问商量以下。然后通知有关执法机构。

一定要记住，除非执法部门的参与，否则你对入侵者进行的一切跟踪都可能是非法的。

4.知会其他有关人员

除了管理者和法律顾问之外，你还需要通知你的恢复工作可能影响到的人员，例如其他网络管理人员和用户。

二、记录恢复过程中所有的步骤

毫不夸张地讲，记录恢复过程中你采取的每一步措施，是非常重要的。恢复一个被侵入的系统是一件很麻烦的事，要耗费大量的时间，因此经常会使人作出一些草率的决定。记录自己所做的每一步可以帮助你避免作出草率的决定，还可以留作以后的参考。记录还可能对法律调查提供帮助。

夺回对系统的控制权

一、将被侵入的系统从网络上断开

为了夺回对被侵入系统的控制权，你需要将其从网络上断开，包括播号连接。断开以后，你可能想进入 U

NIX 系统的单用户模式或者 NT 的本地管理者(local administrator)模式，以夺回系统控制权。然而，重启或者切换到单用户/本地管理者模式，会丢失一些有用的信息，因为被侵入系统当前运行的所有进程都会被杀死。

因此，你可能需要进入“检查网络嗅探器”一节，以确定被侵入的系统是否有网络嗅探器正在运行。

在对系统进行恢复的过程中，如果系统处于 UNIX 单用户模式下，会阻止用户、入侵者和入侵进程对系统的访问或者切换主机的运行状态。

如果在恢复过程中，没有断开被侵入系统和网络的连接，在你进行恢复的过程中，入侵者就可能连接到你的主机，破坏你的恢复工作。

二、复制一份被侵入系统的影象

在进行入侵分析之前，建议你备份被侵入的系统。以后，你可能会用得着。

如果有一个相同大小和类型的硬盘，你就可以使用 UNIX 命令 dd 将被侵入系统复制到这个硬盘。

例如，在一个有两个 SCSI 硬盘的 Linux 系统，以下命令将在相同大小和类型的备份硬盘(/dev/sdb)上复制被侵入系统(在/dev/sda 盘上)的一个精确拷贝。

```
# dd if=/dev/sda of=/dev/sdb
```

还有一些其它的方法备份被侵入的系统。在 NT 系统中没有类似于 dd 的内置命令，你可以使用一些第三方的程序复制被侵入系统的整个硬盘影象。

建立一个备份非常重要，你可能会需要将系统恢复到侵入刚被发现时的状态。它对法律调查可能有帮助。记录下备份的卷标、标志和日期，然后保存到一个安全的地方以保持数据的完整性。

入侵分析

现在你可以审查日志文件和系统配置文件了，检查入侵的蛛丝马迹，入侵者对系统的修改，和系统配置的脆弱性。

一、检查入侵者对系统软件和配置文件的修改

校验系统中所有的二进制文件

在检查入侵者对系统软件和配置文件的修改时，一定要记住:你使用的校验工具本身可能已经被修改过，操作系统的内核也有可能被修改了，这非常普遍。因此，建议你使用一个可信任的内核启动系统，而且你使用的所有分析工具都应该是干净的。对于 UNIX **系统，你可以通过建立一个启动盘，然后对其写保护来获得一个可以信赖的操作系统内核。**

你应该彻底检查所有的系统二进制文件，把它们与原始发布介质(例如光盘)做比较。因为现在已经发现了大量的特洛伊木马二进制文件，攻击者可以安装到系统中。

在 UNIX **系统上，通常有如下的二进制文件会被特洛伊木马代替：**telnet、in.telnetd、login、su、ftp、ls、ps、netstat、ifconfig、find、du、df、libc、sync、inetd **和** syslogd**。除此之外，你还需要检查所有被**/etc/inetd.conf **文件引用的文件，重要的网络和系统程序以及共享库文件。**

在 NT **系统上。特洛伊木马通常会传播病毒，或者所谓的"远程管理程序"，例如** Back Orifice **和** NetBus**。特洛伊木马会取代处理网络连接的一些系统文件。**

一些木马程序具有和原始二进制文件相同的时间戳和 sum **校验值，通过校验和无法判断文件是否被修改。**

因此，对于 UNIX 系统，我们建议你使用 cmp 程序直接把系统中的二进制文件和原始发布介质上对应的文件进行比较。

你还可以选择另一种方法检查可疑的二进制文件。向供应商索取其发布的二进制文件的 MD5 校验值，然后使用 MD5 校验值对可疑的二进制文件进行检查。这种方法适用于 UNIX 和 NT。

校验系统配置文件

在 UNIX 系统中，你应该进行如下检查：

检查/etc/passwd 文件中是否有可疑的用户

检查/etc/inet.conf 文件是否被修改过

如果你的系统允许使用 r 命令,例如 rlogin、rsh、rexec，你需要检查/etc/hosts.equiv 或者.rhosts 文件。

检查新的 SUID 和 SGID 文件。下面命令会打印出系统中的所有 SUID 和 SGID 文件：

```
#find / ( -perm -004000 -o -perm -002000 ) -type f -print
```

对于 NT，你需要进行如下检查：

检查不成对的用户和组成员

检查启动登录或者服务的程序的注册表入口是否被修改

检查"net share"命令和服务器管理工具共有的非验证隐藏文件

检查 pulist.ext 程序无法识别的进程

二、检查被修改的数据

入侵者经常会修改系统中的数据。所以建议你对 web 页面文件、ftp 存档文件、用户目录下的文件以及其它的文件进行校验。

三、检查入侵者留下的工具和数据

入侵者通常会在系统中安装一些工具，以便继续监视被侵入的系统。

入侵者一般会在系统中留下如下种类的文件：

网络嗅探器

网络嗅探器就是监视和记录网络行动的一种工具程序。入侵者通常会使用网络嗅探器获得在网络上以明文进行传输的用户名和密码。

嗅探器在 UNIX 系统中更为常见。

特洛伊木马程序

特洛伊木马程序能够在表面上执行某种功能，而实际上执行另外的功能。因此，入侵者可以使用特洛伊木马程序隐藏自己的行为，获得用户名和密码数据，建立后门以便将来对系统在此访问被侵入系统。

后门

后门程序将自己隐藏在被侵入的系统，入侵者通过

它就能够不通过正常的系统验证，不必使用安全缺陷攻击程序就可以进入系统。

安全缺陷攻击程序

系统运行存在安全缺陷的软件是其被侵入的一个主要原因。入侵者经常会使用一些针对已知安全缺陷的攻击工具，以此获得对系统的非法访问权限。这些工具通常会留在系统中，保存在一个隐蔽的目录中。

入侵者使用的其它工具

以上所列无法包括全部的入侵工具，攻击者在系统中可能还会留下其它入侵工具。这些工具包括：

系统安全缺陷探测工具

对其它站点发起大规模探测的脚本

发起拒绝服务攻击的工具

使用被侵入主机计算和网络资源的程序

入侵工具的输出

你可能会发现入侵工具程序留下的一些日志文件。在这些文件中可能会包含被牵扯的其它站点，攻击者利用的安全缺陷，以及其它站点的安全缺陷。

因此，建议你对系统进行彻底的搜索，找出上面列出的工具及其输出文件。一定要注意：在搜索过程中，要使用没有被攻击者修改过的搜索工具拷贝。

搜索主要可以集中于以下方向：

检查 UNIX 系统/dev/目录下意外的 ASCII 文件。一些特洛伊木马二进制文件使用的配置文件通常在/dev 目录中。

仔细检查系统中的隐藏文件和隐藏目录。如果入侵者在系统中建立一个一个新的帐户，那么这个新帐户的起始目录以及他使用的文件可能是隐藏的。

检查一些名字非常奇怪的目录和文件，例如:...(三个点)、..(两个点)以及空白(在 UNIX 系统中)。入侵者通常会在这样的目录中隐藏文件。对于 NT，应该检查那些名字和一些系统文件名非常接近的目录和文件。

四、审查系统日志文件

详细地审查你的系统日志文件，你可以了解系统是如何被侵入的，入侵过程中，攻击者执行了哪些操作，以及哪些远程主机访问了你的主机。通过这些信息，你能够对入侵有更加清晰的认识。

记住:系统中的任何日志文件都可能被入侵者改动过。

对于 UNIX 系统，你可能需要查看/etc/syslog.conf 文件确定日志信息文件在哪些位置。NT 通常使用三个日志文件，记录所有的 NT 事件，每个 NT 事件都会被记录到其中的一个文件中，你可以使用 Event Viewer 查看日志文件。其它一些 NT 应用程序可能会把自己的日志放到其它的地方，例如 ISS 服务器默认的日志目录是 c:winntsystem32logfiles。

以下是一个通常使用的 UNIX 系统日志文件列表。由于系统配置的不同可能你的系统中没有其中的某些文件。

messages

messages 日志文件保存了大量的信息。可以从这个文件中发现异常信息，检查入侵过程中发生了哪些事情。

xferlog

如果被侵入系统提供 FTP 服务，xferlog 文件就会记录下所有的 FTP 传输。这些信息可以帮助你确定入侵者向你的系统上载了哪些工具，以及从系统下载了哪些东西。

utmp

保存当前登录每个用户的信息，使用二进制格式。这个文件只能确定当前哪些用户登录。使用 who 命令可以读出其中的信息。

wtmp

每次用户成功的登录、退出以及系统重启，都会在 wtmp 文件中留下记录。这个文件也使用二进制格式，你需要使用工具程序从中获取有用的信息。last 就是一个这样的工具。它输出一个表，包括用户名、登录时间、发起连接的主机名等信息，详细用法可以使用 man last 查询。检查在这个文件中记录的可疑连接，可以帮助你确定牵扯到这起入侵事件的主机，找出系统中的哪些帐户可能被侵入了。

secure

某些些版本的 UNIX 系统(例如：RedHat Linux)会将 tcp_wrappers 信息记录到 secure 文件中。如果系统的 inetd 精灵使用 tcp_wrappers,每当有连接请求超出了 inetd 提供的服务范围，就会在这个文件中加入一条日志信息。通过检查这个日志文件，可以发现一些异常服务请求，或者从陌生的主机发起的连接。

审查日志，最基本的一条就是检查异常现象。

五、检查网络嗅探器

入侵者侵入一个 UNIX 系统后，为了获得用户名和

密码信息，一般会在系统上安装一个网络监视程序，这种程序就叫作嗅探器或者数据包嗅探器。对于 NT，入侵者会使用远程管理程序实现上述目的。

判断系统是否被安装了嗅探器，首先要看当前是否有进程使你的网络接口处于混杂（Promiscuous）模式下。如果任何网络接口处于 promiscuous 模式下，就表示可能系统被安装了网络嗅探器。注意如果你重新启动了系统或者在单用户模式下操作，可能无法检测到 Promiscuous 模式。使用 ifconfig 命令就可以知道系统网络接口是否处于 promoscuous 模式下(注意一定使用没有被侵入者修改的 ifconfig):

#/path-of-clean-ifconfig/ifconfig -a

有一些工具程序可以帮助你检测系统内的嗅探器程序：

cpm(Check Promiscuous Mode)--UNIX

可以从以下地址下载：ftp://coast.cs.purdue.edu/pub/tools/unix/cpm/

ifstatus--UNIX

可以从以下地址下载：ftp://coast.cs.purdue.edu/pub/tools/unix/ifstatus/

neped.c

可以从以下地址下载：ftp://apostols.org/AposTolls/snoapshots/neped/neped.c

一定要记住一些合法的网络监视程序和协议分析程序也会把网络接口设置为 promiscuous 模式。检测到网络接口处于 promicuous 模式下，并不意味着系统中有嗅

探器程序正在运行。

但是，在 Phrack 杂志的一篇文章:(Phrack Magazine Volume 8,Issue 53 July 8,1998,article 10 of 15, Interface Promiscuity Obscurity)中,有人提供了一些针对 FreeBSD、Linux、HP-UX、IRIX 和 Solaris 系统的模块，可以擦除 IFF_PROMISC 标志位，从而使嗅探器逃过此类工具的检查。以此，即使使用以上的工具，你没有发现嗅探器，也不能保证攻击者没有在系统中安装嗅探器。

现在，LKM(Loadable Kernel Model,可加载内核模块)的广泛应用，也增加了检测难度。关于这一方面的检测请参考使用 KSAT 检测可加载内核模块。

还有一个问题应该注意，嗅探器程序的日志文件的大小会急剧增加。使用 df 程序查看文件系统的某个部分的大小是否太大，也可以发现嗅探器程序的蛛丝马迹。建议使用 lsof 程序发现嗅探器程序打开的日志文件和访问访问报文设备的程序。在此，还要注意:使用的 df 程序也应该是干净的。

一旦在系统中发现了网络嗅探器程序，我们建议你检查嗅探器程序的输出文件确定哪些主机受到攻击者威胁。被嗅探器程序捕获的报文中目的主机将受到攻击者的威胁，不过如果系统的密码是通过明文传输，或者目标主机和源主机互相信任，那么源主机将受到更大的威胁。

通常嗅探器程序的日志格式如下：

-- TCP/IP LOG -- TM: Tue Nov 15 15:12:29 --

PATH: not_at_risk.domain.com(1567) => at_risk.domain.com(telnet)

使用如下命令可以从嗅探器程序的日志文件中得到

受到威胁的主机列表：

```
% grep PATH: $sniffer_log_file | awk '{print $4}' |
awk -F( '{print $1}'| sort -u
```

你可能需要根据实际情况对这个命令进行一些调整。一些嗅探器程序会给日志文件加密，增加了检查的困难。

你应该知道不只是在嗅探器程序日志文件中出现的主机受到攻击者的威胁，其它的主机也可能受到威胁。

建议你参考 http://www.cert.org/advisories/CA-94.01.ongoing.network.monitoring.attacks.html 获得更为详细的信息。

六、检查网络上的其它系统

除了已知被侵入的系统外，你还应该对网络上所有的系统进行检查。主要检查和被侵入主机共享网络服务(例如:NIX、NFS)或者通过一些机制(例如：hosts.equiv、.rhosts 文件，或者 kerberos 服务器)和被侵入主机相互信任的系统。

建议你使用 CERT 的入侵检测检查列表进行这一步检查工作。

http://www.cert.org/tech_tips/intruder_detection_checklist.html

http://www.cert.org/tech_tips/win_intruder_detection_checklist.html

七、检查涉及到的或者受到威胁的远程站点

在审查日志文件、入侵程序的输出文件和系统被侵入以来被修改的和新建立的文件时，要注意哪些站点可能会连接到被侵入的系统。根据经验那些连接到被侵入

主机的站点，通常已经被侵入了。所以要尽快找出其它可能遭到入侵的系统，通知其管理人员。

通知相关的 CSIRT 和其它被涉及的站点

一、事故报告

入侵者通常会使用被侵入的帐户或者主机发动对其它站点的攻击。如果你发现针对其它站点的入侵活动，建议你马上和这些站点联络。告诉他们你发现的入侵征兆，建议他们检查自己的系统是否被侵入，以及如何防护。要尽可能告诉他们所有的细节，包括：日期/时间戳、时区，以及他们需要的信息。

你还可以向 CERT(计算机紧急反应组)提交事故报告，从他们那里的到一些恢复建议。

中国大陆地区的网址是: http://www.cert.org.cn

二、与 CERT 调节中心(CERT Coordination Center)联系

你还可以填写一份事故报告表，使用电子邮件发送到 http://www.cert.org,从那里可以得到更多帮助。CERT 会根据事故报告表对攻击趋势进行分析，将分析结果总结到他们的安全建议和安全总结,从而防止攻击的蔓延。可以从以下网址获得事故报告表：

http://www.cert.org/ftp/incident_reporting_form

三、获得受牵连站点的联系信息

如果你需要获得顶级域名(.com、.edu、.net、.org 等)的联系信息，建议你使用 interNIC 的 whois 数据库：http://rs.internic.net/whois.html。

如果你想要获得登记者的确切信息，请使用 interNIC 的登记者目录：http://rs.internic.net/origin.html。

想获得亚太地区和澳洲的联系信息，请查询：http:

//www.apnic.net/apnic-bin/whois.pl，http://www.aunic.net/cgi-bin/whois.aunic

如果你需要其它事故反应组的联系信息，请查阅 FIRST(Forum of Incident Response and Security Teams)的联系列表：http://www.first.org/team-info/

要获得其它的联系信息，请参考：http://www.cert.org/tech_tips/finding_site_contacts.html

建议你和卷入入侵活动的主机联系时，不要发信给 root 或者 postmaster。因为一旦这些主机已经被侵入，入侵者就可能获得了超级用户的权限，就可能读到或者拦截送到的 e-mail。

恢复系统

一、安装干净的操作系统版本

一定要记住如果主机被侵入，系统中的任何东西都可能被攻击者修改过了，包括：内核、二进制可执行文件、数据文件、正在运行的进程以及内存。通常，需要从发布介质上重装操作系统，然后在重新连接到网络上之前，安装所有的安全补丁，只有这样才会使系统不受后门和攻击者的影响。只是找出并修补被攻击者利用的安全缺陷是不够的。

我们建议你使用干净的备份程序备份整个系统。然后重装系统。

二、取消不必要的服务

只配置系统要提供的服务，取消那些没有必要的服务。检查并确信其配置文件没有脆弱性以及该服务是否可靠。通常，最保守的策略是取消所有的服务，只启动你需要的服务。

三、安装供应商提供的所有补丁

我们强烈建议你安装了所有的安全补丁，要使你的系统能够抵御外来攻击，不被再次侵入，这是最重要的一步。

你应该关注所有针对自己系统的升级和补丁信息。

四、查阅 CERT 的安全建议、安全总结和供应商的安全提示

我们鼓励你查阅 CERT 以前的安全建议和总结，以及供应商的安全提示，一定要安装所有的安全补丁。

CERT 安全建议：http://www.cert.org/advisories/

CERT 安全总结：http://www.cert.org/advisories/

供应商安全提示：ftp://ftp.cert.org/pub/cert_bulletins/

五、谨慎使用备份数据

在从备份中恢复数据时，要确信备份主机没有被侵入。一定要记住，恢复过程可能会重新带来安全缺陷，被入侵者利用。如果你只是恢复用户的 home 目录以及数据文件，请记住文件中可能藏有特洛伊木马程序。你还要注意用户起始目录下的.rhost 文件。

六、改变密码

在弥补了安全漏洞或者解决了配置问题以后，建议你改变系统中所有帐户的密码。一定要确信所有帐户的密码都不容易被猜到。你可能需要使用供应商提供的或者第三方的工具加强密码的安全。

加强系统和网络的安全

一、根据 CERT 的 UNIX/NT 配置指南检查系统的安全性

CERT 的 UNIX/NT 配置指南可以帮助你检查系统中

容易被入侵者利用的配置问题。

http://www.cert.org/tech_tips/unix_configuration_guidelines.html

http://www.cert.org/tech_tips/win_configuration_guidelines.html

二、查阅安全工具文档

可以参考以下文章，决定使用的安全工具：http://www.cert.org/tech_tips/security_tools.html

三、安装安全工具

在将系统连接到网络上之前，一定要安装所有选择的安全工具。同时，最好使用 Tripwire、aide 等工具对系统文件进行 MD5 校验，把校验码放到安全的地方，以便以后对系统进行检查。

四、打开日志

启动日志(logging)/检查(auditing)/记帐(accounting)程序,将它们设置到准确的级别,例如 sendmail 日志应该是 9 级或者更高。经常备份你的日志文件，或者将日志写到另外的机器、一个只能增加的文件系统或者一个安全的日志主机。

五、配置防火墙对网络进行防御

现在有关防火墙的配置文章很多，在此就不一一列举了。你也可以参考：http://www.cert.org/tech_tips/packet_filtering.html

重新连接到 Internet

完成以上步骤以后，你就可以把系统连接回 Internet 了。

升级你的安全策略

CERT 调节中心建议每个站点都要有自己的计算机安全策略。每个组织都有自己特殊的文化和安全需求，因此需要根据自己的情况指定安全策略。关于这一点请参考 RFC2196 站点安全手册: ftp://ftp.isi.edu/in-notes/rfc2196.txt

一、总结教训

从记录中总结出对于这起事故的教训，这有助于你检讨自己的安全策略。

二、计算事故的代价

许多组织只有在付出了很大代价以后才会改进自己的安全策略。计算事故的代价有助于让你的组织认识到安全的重要性。而且可以让管理者认识到安全有多么重要。

三、改进你的安全策略

最后一步是对你的安全策略进行修改。所做的修改要让组织内的所有成员都知道，还要让他们知道对他们的影响。

Windows 2000 中的网际协议安全(IPSec)

网际协议安全(IPSec)

网际协议安全 (IPSec) 可以对专用网络和 Internet 攻击的主动保护，同时保持易用性。 并且，它是一套基于加密术的保护服务以及安全协议。

它采用端对端的安全保护模式，保护工作组、局域网计算机、域客户和服务器、距离很远的分公司、Extr

anet、漫游客户以及远程管理计算机间通讯的能力。

IPSec 作为安全网络的长期方向，是基于密码学的保护服务和安全协议的套件。因为它不需要更改应用程序或协议，您可以很容易地给现有网络部署 IPSec。

Windows 2000 的 IPSec 实现基于 Internet 工程任务组 (IETF) IPSec 工作组开发的工业标准。

Windows2000 的安全策略模式

更为强大的基于加密术的安全方法可能导致大幅度增加管理开销。Windows 2000 通过实现基于策略的网际协议安全 (IPSec) 管理避免了该缺陷。

可以使用策略而非应用程序或操作系统来配置 IPSec 。网络安全管理员可以配置多种 IPSec 策略，从单台计算机到 Active Directory 域、站点或组织单位。Windows 2000 提供集中管理控制台、IP 安全策略管理来定义和管理 IPSec 策略。在大多数已有网络中，可以配置这些策略为大多数交通类型提供各种级别的保护。

IPSec 的数据保护方式

因为网络攻击可能导致系统停工、生产力损失和敏感数据的公开暴露，所以保护信息不被未经授权的第三方破译或修改是高度优先的事情。

网络保护策略一般都是集中在周界安全方面，通过使用防火墙、安全网关和拨号访问的用户身份验证来防止来自私有网外部的攻击。然而，它并不保护不受来自网络内部的攻击。

只集中在访问控制安全性（例如使用智能卡和 Kerberos）可能不会带来全面的保护，因为这些方法依赖于用户名和密码。有许多计算机是由多个用户共享使用的，由于它经常处于已登录状态而导致计算机的不安全。另

外，如果一个用户名或密码已被攻击者截获，单单基于访问控制的安全性不会防止非法访问网络资源。

物理级的保护策略通常不使用，它保护物理的网线和访问点不被使用。然而，这好象不大可能保证整个网络路径的安全得到保护，因为数据将不得不从源到目的地传播。

一个完善的安全计划包含多个安全策略以获得深度的保护。其中的任何一个策略都可以和 IPSec 结合。这就通过保证发送端计算机在传输前，也就是每个 IP 数据包到达网线之前对其实施保护，而接收端计算机只有在数据被接收和验证之后再解除对数据的保护，从而提供了另一层安全性。

网络安全

在 IP 传输层（网络层 3）实现 IPSec 会启用开销很小的高级保护。配置使用 IPSec 不需要更改已有的应用程序或操作系统。可以配置 IPSec 用于已有的企业方案，例如：工作组；局域网 (LAN)：客户/服务器，对等网；远程访问：漫游客户、Internet 访问、Extranet、远程办事处。

其他在网络层 3 以上运行的安全机制（例如安全套接层，SSL）仅保护会使用 SSL 的应用程序，例如 Web 浏览器。必须修改所有其他的应用程序以使用 SSL 保护通讯。其他在网络层 3 以下运行的安全机制（例如链接层加密）仅保护该链接，而不必保护数据路径上的所有链接。这使得链接层加密无法适用于 Internet 或路由 Intranet 方案上的端对端数据保护。

在网络层 3 上执行的 IPSec 保护 TCP/IP 协议簇中所有 IP 和更高层的协议，例如 TCP、UDP、ICMP、

Raw（协议 255），甚至保护在 IP 层上发送通讯的自定义协议。保护此层信息的主要好处是所有使用 IP 传输数据的应用程序和服务均可以使用 IPSec 保护，而不必修改这些应用程序和服务。（要保护非 IP 协议，数据包必须由 IP 封装。）

IPSec 的密钥保护

IPSec 保护数据将让攻击者感到破解相当困难或根本不可能。算法和密钥的组合用于保护信息。通过使用基于加密的算法和密钥获得高安全级。算法是用来保护信息的数学过程，密钥是需要读取、修改或验证所保护数据的密码或数字。

IPSec 使用以下特性大幅度地阻止并减少网络攻击：

自动密钥管理

密钥生成

要启用安全通讯，两台计算机必须可以建立相同的共享密钥，而不能通过网络在相互之间发送密钥。IPSec 使用 Diffie-Hellman 算法启用密钥交换，并为所有其他加密密钥提供加密材料。

两台计算机启动 Diffie-Hellman 计算，然后公开或秘密（使用身份验证)交换中间结果。计算机从来不发送真正的密钥。通过使用来自交换的共享信息，每台计算机都生成相同的密钥。专家级用户可以修改默认密钥交换及数据加密密钥设置。

密钥长度

每当密钥的长度增加一位，可能的密钥数会加倍，破解密钥的难度也会成倍加大。两台计算机之间的 IPSec 安全协商生成两种类型的共享密钥：主密钥和会话密

钥。主密钥很长，有 768 位或 1023 位。主密钥用作会话密钥的源。会话密钥由主密钥通过一种标准方法生成，每种加密和完整性算法都需要会话密钥。

如何管理会话密钥——密钥交换

保护密钥交换阶段的密钥的强度通过以下特性被增强：

1、密钥生命期

生命期设置决定何时生成新密钥。任何时候当密钥的生命期到达时，相关的 SA 也将重新协商。在一定的时间间隔内重新生成新的密钥的过程被称为动态重新生成密钥或密钥重新生成。生命期允许您在一定的时间间隔后强制生成（重新生成）新的密钥。例如，如果通讯需要 100 分钟并且您指定的密钥生命期为 10 分钟，那么，在交换的过程中将生成 10 个密钥，每 10 分钟一个。使用多个密钥保证了即使攻击者获得了一部分通讯的密钥，也不会危及全部通讯的安全。密钥的自动重新生成由默认设置提供。专家级用户可以覆盖默认值，通过会话密钥或“完整转寄保密”指定一个主密钥生命期（以分钟为单位）。

设置不同的密钥生命期时应倍加小心，因为他们也将决定 SA 的生命期。例如，设置主密钥生命期为 8 小时（480 分钟），会话生命期（在“筛选器操作”中设置）为 2 小时将导致在 ISAKMP SA 过期后 IPSec SA 仍保留 2 小时。如果新的 IPSec SA 正好在 ISAKMP SA 过期前生成，就会发生这种情况。

2、会话密钥限制

再三地从相同的主密钥重新生成密钥将最终危及该密钥的安全。例如，假如计算机 A 上的 Bob 发送一条

消息给计算机 B 上的 Alice，然后过了几分钟又发送一条消息给 Alice，由于与该计算机刚建立安全关系，相同的密钥材料可以重用。如想限制该重用次数，专家级用户可以指定一个会话密钥限制。

注意，如果您决定启用主密钥的“完整转寄保密”，会话密钥限制将被忽略；PFS 每次都强制重新生成密钥。例如，启用主密钥的“完整转寄保密”相当于将会话密钥限制指定为 1。

请注意，如果您既指定主密钥生命期（以分钟为单位），又指定会话密钥限制，任何一个首先到达的时间间隔将触发新的密钥。

3、主密钥“完整转寄保密”(PFS)

确定新密钥是如何生成的。启用 PFS 保证密钥被用来保护传输，而无论在哪个阶段都不能够被用于生成其他的密钥。另外，密钥的密钥材料不能用来生成任何新的密钥。

应小心使用主密钥 PFS，因为它需要重新进行身份验证。对于网上的域控制器来说，这可能导致额外的开销。这并不需要在两端都启用。

配置密钥交换

1. 在“IP 安全策略管理”中，右键单击要修改的策略，然后单击“属性”。

2. 单击“常规”选项卡，然后单击“高级”。

3. 要强制重新加密每个会话密钥的主密钥，请单击“主密钥完全向前保密”。

4. 如果需要不同的设置，可在“身份验证和生成新密钥间隔（以分钟计）”中输入一个值，这将导致在该间隔中重新进行身份验证和生成新密钥。

5. 如果需要不同的设置，可在“身份验证和生成新密钥间隔（以会话计）”中输入一个值，以设置重复使用主密钥或其基本密钥材料生成会话密钥的最大次数限制。达到该限制值时将强制进行身份验证和新密钥生成。

6. 如果对密钥交换安全措施有特殊需求，可单击“方法”。

创建密钥交换方法

1. 在“IP 安全策略管理”中，右键单击要修改的策略，然后单击“属性”。

2. 单击“常规”，单击“高级”选项卡，再单击“方法”。

3. 单击“添加”，如果正重新配置现存的方法，请单击该安全措施，然后单击“编辑”。

4. 选择一种“完整性算法”：

o 单击“MD5”使用 128 位值。

o 单击“SHA”使用 160 位值（更强）。

5. 选择一种“加密算法”：

o 单击“3DES”使用最高的安全算法。

o 如果要连接到不具有 3DES 功能的计算机，或者不需要更高的安全性和 3DES 的开销，请单击“DES”。有关加密设置的详细信息，请参阅“特殊考虑”。

6. 选择“Diffie-Hellman 小组”，设置要用于生成实际密钥的基本密钥材料的长度：

o 单击“低 (1)”使用 768 位作为基础。

o 单击“中 (2)”使用 1024 位作为基础（更强）。

动态重生成密钥

IPSec 可以在通讯的过程中自动生成新的密钥。这样可以防止攻击者只用一个破解的密钥就能获得完整的通讯数据。专家级用户可以修改默认的加密时间间隔。

安全服务

完整性

完整性保护信息在传输过程中免遭未经授权的修改，从而保证接收到的信息与发送的信息完全相同。数学散列函数用来唯一地标记或“签发”每个包。接收端的计算机在打开包之前检查签名。如果签名改变（因而，数据包当然也改变），数据包就会被丢弃以防止可能的网络攻击。

身份验证

身份验证通过保证每个计算机的真实身份来检查消息的来源以及完整性。没有可靠的身份验证，不明来历的计算机发送的任何信息都是不可信的。在每一项策略中都会列出多种身份验证方法，以保证 Windows 2000 域成员、没有运行 Windows 2000 的计算机及远程计算机都能找到一个通用的身份验证方法。

机密性（数据加密）

机密性保证只有预期的接收者才能读出数据。当选择该特性后，将使用 IPSec 数据包的封装安全负载 (ESP) 格式。数据包在传输之前先加密，确保其在传输过程中即使被攻击者监视或截取也不会暴漏。只有具有共享密钥的计算机能够解释或修改数据。美国数据加密标准 (DES) 算法 DES 和 3DES 可提供安全协商和应用程序数据交换两方面的保密性。密码数据块链 (CBC) 用于隐藏数据包中数据块的模式，加密后不增加数据的大小。重复的加密模式可能为攻击者提供解开密钥的线

索，从而使安全性受到威胁。初始化向量（一个初始的随机数）可用作加密或解密数据块的第一个随机块。不同的随机块可与密钥结合使用，以便加密每个块。这将保证相同的不安全数据集被转换为不同的加密数据集。

认可

保证邮件的发件人只能是发送该邮件的人；发送者不能抵赖曾经发送过该邮件。

反重发

又称作禁止重发，它保证每个 IP 包的唯一性。由攻击者捕获的邮件不能被重用或重发以非法建立会话或获取信息。

Cisco 路由器如何防止 DDoS 攻击

使用 ip verfy unicast reverse-path 网络接口命令

这个功能检查每一个经过路由器的数据包。在路由器的 CEF（Cisco Express Forwarding）表该数据包所到达网络接口的所有路由项中，如果没有该数据包源 IP 地址的路由，路由器将丢弃该数据包。例如，路由器接收到一个源 IP 地址为 1.2.3.4 的数据包，如果 CEF 路由表中没有为 IP 地址 1.2.3.4 提供任何路由（即反向数据包传输时所需的路由），则路由器会丢弃它。

单一地址反向传输路径转发（Unicast Reverse Path Forwarding）在 ISP（局端）实现阻止 SMURF 攻击和

其它基于 IP 地址伪装的攻击。这能够保护网络和客户免受来自互联网其它地方的侵扰。使用 Unicast RPF 需要打开路由器的"CEF swithing"或"CEF distributed s

witching"选项。不需要将输入接口配置为 CEF

交换（switching）。只要该路由器打开了 CEF 功能，所有独立的网络接口都可以配置为其它交换（switching）模式。RPF（反向传输路径转发）属于在一个网络接口或子接口上激活的输入端功能，处理路由器接收的数据包。

在路由器上打开 CEF 功能是非常重要的，因为 RPF 必须依靠 CEF。Unicast RPF 包含在支持 CEF 的 Cisco IOS 12.0 及以上版本中，但不支持 Cisco IOS 11.2 或 11.3 版本。

2、使用访问控制列表（ACL）过滤 RFC 1918 中列出的所有地址

参考以下例子：

```
interface xy
ip access-group 101 in
access-list 101 deny ip 10.0.0.0 0.255.255.255 any

access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 permit ip any any
```

3、参照 RFC 2267，使用访问控制列表（ACL）过滤进出报文

参考以下例子：

{ISP 中心} -- ISP 端边界路由器 -- 客户端边界路由器 -- {客户端网络}

ISP 端边界路由器应该只接受源地址属于客户端网

络的通信，而客户端网络则应该只接受源地址未被客户端网络过滤的通信。以下是 ISP **端边界路由器的访问控制列表（**ACL**）例子：**

access-list 190 permit ip {**客户端网络**} {**客户端网络掩码**} any

access-list 190 deny ip any any [log]

interface {**内部网络接口**} {**网络接口号**}

ip access-group 190 in

以下是客户端边界路由器的 ACL **例子：**

access-list 187 deny ip {**客户端网络**} {**客户端网络掩码**} any

access-list 187 permit ip any any

access-list 188 permit ip {**客户端网络**} {**客户端网络掩码**} any

access-list 188 deny ip any any

interface {**外部网络接口**} {**网络接口号**}

ip access-group 187 in

ip access-group 188 out

如果打开了 CEF **功能，通过使用单一地址反向路径转发（**Unicast RPF**），能够充分地缩短访问控制列表（**ACL**）的长度以提高路由器性能。为了支持** Unicast RPF**，只需在路由器完全打开** CEF**；打开这个功能的网络接口并不需要是** CEF **交换接口。**

4**、使用** CAR**（**Control Access Rate**）限制** ICMP **数据包流量速率**

参考以下例子：

interface xy

rate-limit output access-group 2020 3000000 5120

00 786000 conform-action

transmit exceed-action drop

access-list 2020 permit icmp any any echo-reply

请参阅 IOS Essential Features **获取更详细资料。**

5、**设置** SYN **数据包流量速率**

interface {int}

rate-limit output access-group 153 45000000 1000 00 100000 conform-action

transmit exceed-action drop

rate-limit output access-group 152 1000000 10000 0 100000 conform-action

transmit exceed-action drop

access-list 152 permit tcp any host eq www

access-list 153 permit tcp any host eq www estab lished

在实现应用中需要进行必要的修改，替换：

45000000 **为最大连接带宽**

1000000 **为** SYN flood **流量速率的** 30%**到** 50%**之间的数值。**

burst normal**（正常突变）和** burst max**（最大突变）两个速率为正确的数值。**

注意，如果突变速率设置超过 30%**，可能会丢失许多合法的** SYN **数据包。使用**"show interfaces rate-limit" **命令查看该网络接口的正常和过度速率，能够帮助确定合适的突变速率。这个** SYN **速率限制数值设置标准是保证正常通信的基础上尽可能地小。**

警告：一般推荐在网络正常工作时测量 SYN **数据包流量速率，以此基准数值加以调整。必须在进行测量时**

确保网络的正常工作以避免出现较大误差。

另外，建议考虑在可能成为 SYN 攻击的主机上安装 IP Filter 等 IP 过滤工具包。

6、搜集证据并联系网络安全部门或机构

如果可能，捕获攻击数据包用于分析。建议使用 SUN 工作站或 Linux 等高速计算机捕获数据包。常用的数据包捕获工具包括 TCPDump 和 snoop 等。基本语法为：

```
tcpdump -i interface -s 1500 -w capture_file
snoop -d interface -o capture_file -s 1500
```

本例中假定 MTU 大小为 1500。如果 MTU 大于 1500，则需要修改相应参数。将这些捕获的数据包和日志作为证据提供给有关网络安全部门或机构。

防黑安全模型

一、黑客常用手段

1．黑客攻击的目的

（1）获取目标系统的非法访问

获得不该获得的访问权限。

（2）获取所需资料

包括科技情报、个人资料、金融账户、技术成果、系统信息等等。

（3）篡改有关数据

篡改资料，达到非法目的。

（4）利用有关资源

利用这台机器的资源对其他目标进行攻击，发布虚

假信息，占用存储空间。

2．黑客攻击的方式

（1）远程攻击

指外部黑客通过各种手段，从该子网以外的地方向该子网或者该子网内的系统发动攻击。远程攻击的时间一般发生在目标系统当地时间的晚上或者凌晨时分，远程攻击发起者一般不会用自己的机器直接发动攻击，而是通过跳板的方式，对目标进行迂回攻击，以迷惑系统管理员，防止暴露真实身份。

（2）本地攻击

指本单位的内部人员，通过所在的局域网，向本单位的其他系统发动攻击，在本机上进行非法越权访问也是本地攻击。本地攻击不排除使用跳板的可能。

（3）伪远程攻击

指内部人员为了掩盖攻击者的身份，从本地获取目标的一些必要信息后，攻击过程从外部远程发起，造成外部入侵的现象，从而使追查者误以为攻击者是来自外单位。

3．黑客攻击所采用的途径

黑客之所以能得手，无非是利用了各种安全弱点，其中包括：

（1）管理漏洞

如两台服务器用同一个用户/密码，则入侵了 A 服务器后，B 服务器也不能幸免。

（2）软件漏洞

如 Sun 系统上常用的 Netscape EnterPrise Server 服务，只需输入一个路径，就可以看到 Web 目录下的所有文件清单；又如很多程序只要接收到一些异常或者超长

的数据和参数，就会导致缓冲区溢出。

（3）结构漏洞

比如在某个重要网段由于交换机、集线器设置不合理，造成黑客可以监听网络通信流的数据；又如防火墙等安全产品部署不合理，有关安全机制不能发挥作用，麻痹技术管理人员而酿成黑客入侵事故。

（4）信任漏洞

比如本系统过分信任某个外来合作伙伴的机器，一旦这台合作伙伴的机器被黑客入侵，则本系统的安全受严重威胁。

综上所述，一个黑客要成功入侵系统，必须分析各种和这个目标系统相关的技术因素、管理因素和人员因素。

二、黑客网络攻击的四个层次

1．单元分析

单一目标的系统技术分析。

2．网络分析

与目标有关的网络系统的技术分析。

3．组织分析

与目标有关的组织分析。

4．人物分析

与目标有关的人物分析。

对于外部的黑客而言，所用到的四个攻击层次的比例见图 1。

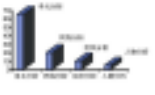


图 1 外部黑客四个层次攻击比例

从图 1 可以看出，单元系统分析所占的比例最大，是黑客攻击的最主要途径。其他三个层次的分析，都是走迂回路线，即通过上游节点和网络邻居，先拿到该系统的有关资料和数据，或者对企业的安全管理漏洞下手，对管理员的不良习惯进行分析，再对该系统进行攻击尝试。在这里人物分析比例最小，因为要获得与系统安全管理有关的人物资料相对而言是最难的，不到不得已时，一般的黑客都不采用。

对于内部黑客而言，在组织分析和人物分析，甚至是网络分析方面，都有着得天独厚的优势，内部黑客会清楚地知道系统管理员是谁，了解到企业内部有多少台服务器，企业和哪些合作伙伴有业务来往，通信和合作机制上是否有漏洞可钻等。对于内部黑客而言，反而是单元系统分析的难度较大。内部黑客所用的四个攻击层次比例见图 2。

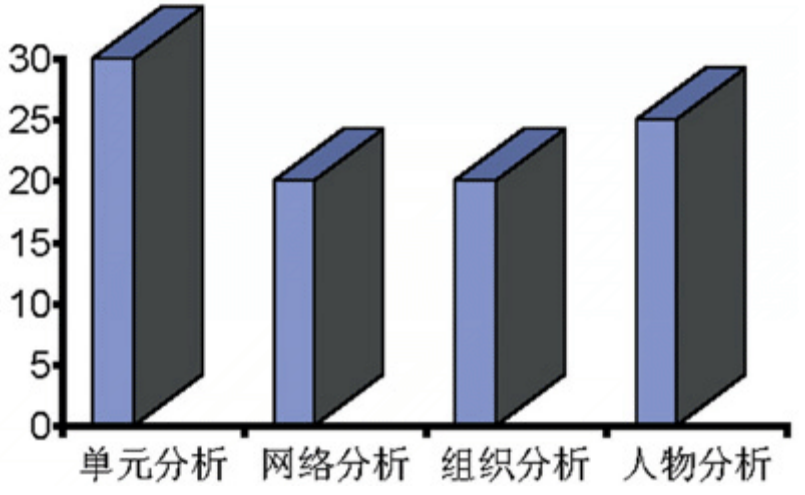


图 2 内部黑客四个层次攻击比例

三、构筑立体防御体系

从上面的分析看出，要想防止内外黑客入侵破坏系统，必须从系统漏洞、网络漏洞、组织管理漏洞和人员安全素质各方面下手。主要目的是：

1．整个系统必须高效正常运作。

2．外来攻击不能使本系统停止运转。

3．内网用户可以较方便地建立、增加服务，设置管理权限。

4．单台主机和设备不存在系统安全漏洞。

5．整个网络不存在结构漏洞和安全突破口。

6．与合作单位的外部通信不受侵犯。

7．合作单位的安全问题不致影响本系统。

8．对非法访问（包括基于协议的和基于内容的）可以及时报警、记录并切断。

9．信息传输安全。

以上第 1、2 点，主要是针对恶意的数据包攻击的防范，可以通过防火墙和安全策略予以实现；第 3～7 点要求比较复杂，首先对安全漏洞和弱点进行检查修补，将网络结构予以优化，可以通过扫描技术、人工分析和系统修复工作予以解决，还将用到访问控制、身份认证等技术；而第 8 点要求对非法信息予以监控，可以通过入侵检测技术实现；第 9 点所提出的信息安全问题，可以通过加密手段予以实现。这些技术不仅仅要用到各种安全产品，还需要有效的服务、培训、部署、安装等。

最后，进行模拟入侵攻击测试，测试安全系统的强壮性，如果再发现问题，再次予以解决。系统的安全强

壮性与模拟入侵测试人员的攻击水平有关。

为了保证所有的安全工具和安全措施得以发挥最大的效果,还有必要对相关人员进行有关的产品售后培训、安全意识培训、安全习惯和机制培训、安全动手技术培训等。

到此为止，完成了网络系统安全的平面部署，可以达到一个理想状态。它暂时是安全的，但随着时间的推移，各种内外因素的变化，该安全系统的安全性将会发生变化。因此，网络安全是相对的，是相对人、系统、应用和时间而言的。

在此基础上，安络的安全专家针对重要系统，金融、政府和电信领域的网络业务，提出了在动态网络安全条件下的动态网络安全解决方案。该方案是一个面向企业的(而非面向社会的)系统工程，是相对时间而言的立体三维结构防御体系，如图 3 所示。

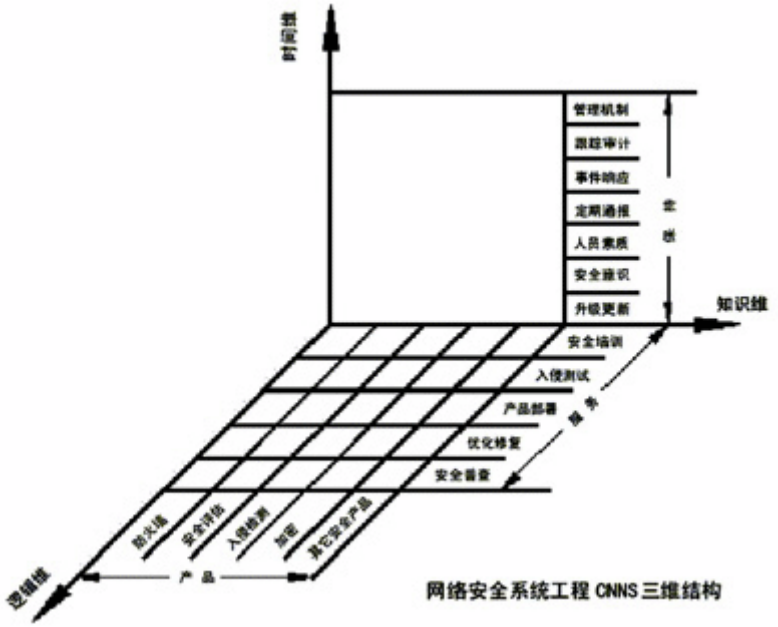


图 3 网络安全系统 CNNS 三维结构

网络安全系统工程 CNNS 三维结构，是根据网络安全系统经过优化可以暂时保持高安全状态，但随着时间的推移安全性将不断降低的特点，提出的一种网络安全系统工程方法实现论。这是国内业界首次建立的网络安全解决方案理论模型。在目前国内几个大型的 ICP、ISP、政府、金融等领域得到了有效的运用，取得了良好的效果。据美国联邦调查局的统计，世界上的信息安全案件中，80%以上是因为系统存在安全漏洞，而遭致内外黑客入侵造成的。该理论模型主要是针对黑客入侵，能与信息安全系统（主要指加密、防病毒等）有良好的衔接。

CNNS 三维结构将整个网络系统安全工程的活动过程分为产品工具库的部署安装、服务的组织和实施步骤等紧密衔接的五个模块和五个阶段，同时还考虑了保持这些活动效果所需要的要素和措施，这样就形成了知识维、逻辑维和时间维所组成的三维空间结构。其中知识维表示实现安全系统所需要的工具库和知识库，逻辑维指知识的有效运用，解决现有安全问题并把现有系统安全状况提升到理想状况所要进行的工作内容和逻辑步骤，而时间维则在特定的一段时间内对保持系统安全需要所进行的工作。知识维和逻辑维组成的平面，可以把系统的安全状况提升到当前安全技术所能达到的理想状态，而时间维则对这个安全状态予以保持。由于网络安全技术和黑客技术日新月异，每年世界网络安全形势会有较大的变化，而每年度企业内部对网络应用一般都会有新的规划，因此整个立体解决方案的最佳时效为一年。

一年之后，可再根据此模型对整个系统安全重新分析，必要时可以重复知识维和逻辑维组成的平面工程。

局域网的安全策略

Internet 是目前世界上最为开放的计算机网络系统。相对于我们的现实生活世界来讲，也可以把它称作为电脑空间。和现实生活世界一样，在电脑空间当中也仍然存在着各种各样的网络犯罪问题，如用非法的手段窃取秘密数据，破坏系统，恶意欺骗等。因此你必须时刻防范来自 Internet 的恶意攻击，关注你局域网的计算机系统安全。

在这篇文章里我们谈一谈网络攻击的机制，同时也着重讲述一下局域网系统避免遭受攻击的方法。

和现实世界一样，由于 Internet 上的攻击和恐吓经常是有计划发生的，所以我们可以通过某些途径，利用某些手段，预知某一次或某一类攻击的发生。

这里我们使用网络协议分层模式来分析局域网的安全。从图 1 我们可以看到，网络的七层在不同程度上会遭受到不同方式的攻击，如果攻击者取得成功，那将是非常危险的。而我们通常听到或见到的攻击往往发生在应用层，这些攻击主要是针对 Web 服务器、浏览器和他们访问到的信息，比较常见的还有攻击开放的文件系统部分。

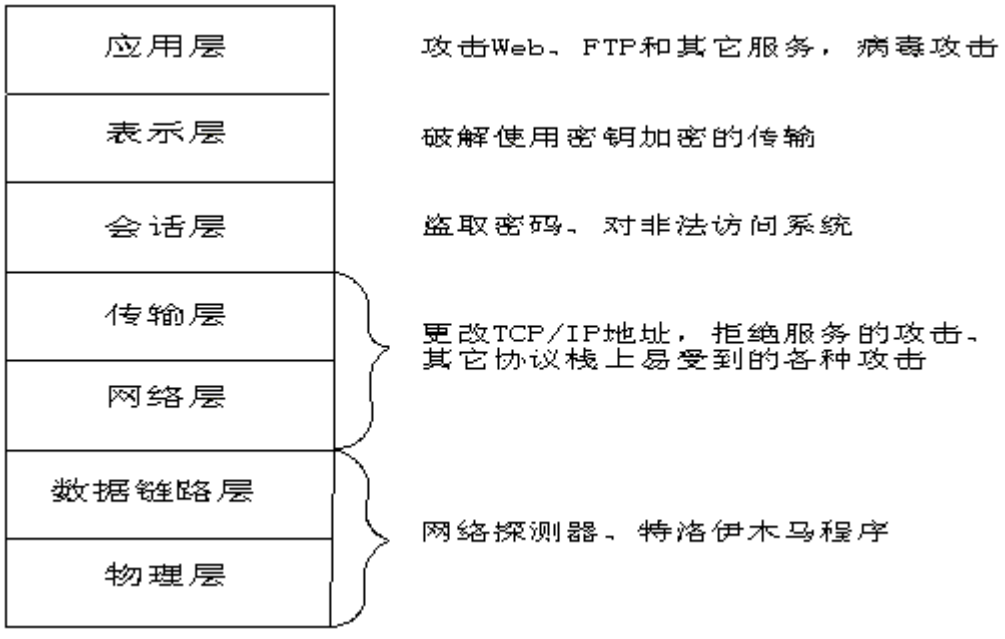


图 1 七层模型易遭受的安全攻击

到目前为止，人们还没有找到防范七层模型受到全部攻击的措施。但下面两个方法从实践上来说被认为是非常有用的防范手段。

1、 包过滤

你可以在网络层检查通信数据，观察它的源地址和目的地址。过滤器可以禁止特定的地址或地址范围传出或进入，也可以禁止令人怀疑的地址模式。

2、 防火墙

你可以在应用层检查通信数据，检查消息地址中的端口，或检查特定的应用的消息内容。测试失败的任何通信数据将被拒绝。

下面我们要谈的是包过滤和防火墙安全实施的不同

方法。

一、路由包过滤

TCP/IP 地址由机器地址和标识程序处理消息的端口数字组成。这个地址/端口组合信息对每个 TCP/IP 消息都是有效的。包过滤与防火墙相比处理的简单一些，它仅是观察 TCP/IP 地址，而不是端口数字或消息内容。不过包过滤提供给你的是很好的网络安全工具。

包过滤器通常使用的是自顶向下的操作原则，下面是它使用的一个典型规则：

1、 允许所有传出通信数据的通过；

2、 拒绝建立新的传入连接；

3、 其它的数据可以全部被接受；

通过这样的使用规则，系统的安全性提高了许多。因为它拒绝了 Internet 上主动与你的计算机建立新的连接的请求。它阻止使用 TCP 的通信数据进入，从而杜绝了对共享驱动器和文件的未授权访问。包过滤使用这样的模式对用户来说有很大意义，它打破了 FTP 客户和服务器之间的正常操作，因为这样的模式需要服务器在开始传输时对连接进行初始化。实际上现在所有的 FTP 软件都支持 PASV 模式，这是为解决上面的问题而专门设计的。通过设置客户为“请求 PASV 模式”，你可以使所有的连接被客户初始化。

过滤器通常的应用是配置在连接你的计算机和 Internet 的路由器上，如图 2 所示。在你的局域网和 Internet 之间放置过滤器后，就可以保证局域网与 Internet 所有的通信数据都要经过过滤器。

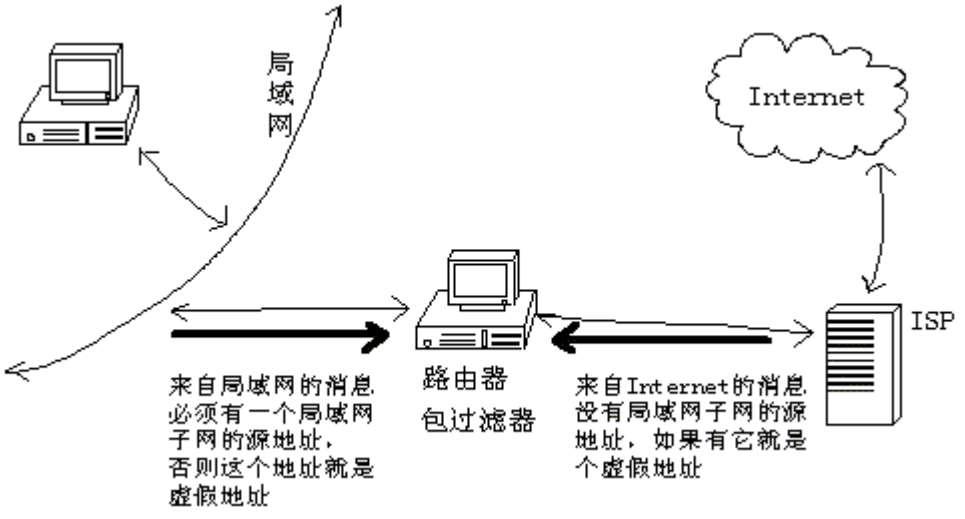


图 2　包过滤器的配置

如果你的包过滤软件有能力检查源地址子网，在子网上物理端口传递消息到路由器，你就可以制定规则来避免虚假的 TCP/IP 地址，就象图 2 所示的那样。攻击者欺骗的方法就是把来自 Internet 的消息伪装成来自你局域网的消息。包过滤通过拒收带有不可能源地址的消息来防御攻击者的攻击。例如，假定你在一个装有 Linux 的机器上安装软件，让它作为一个 Windows 网络文件服务器，你可以配置 Linux 让它拒收所有来自你的子网以外的通信数据，阻止 Internet 上的机器看到这个文件服务器。如果攻击者假装是你内部的机器，用过滤器就可以阻止攻击者的攻击。

包过滤虽然对网络的安全防范能起到很好的作用，但包过滤也并不是万能的。它们一般不能防御使用 UDP 协议的攻击，因为过滤器不能拒收开放的消息。包过滤

还不能防御低层攻击，象 PING 方式的攻击。

二、防火墙

使用防火墙软件可以在一定程度上控制你的局域网和 Internet 之间传递的数据。图 3 所示是一个 TCP/IP 数据包报头示意图，从它上面你可以清楚地看到包过滤和防火墙工作原理的不同之处。防火墙不但检查了包过滤检查内容的所有部分（TCP/IP 的源地址和目的地址），还检查了源/目的端口数字和包的内容。

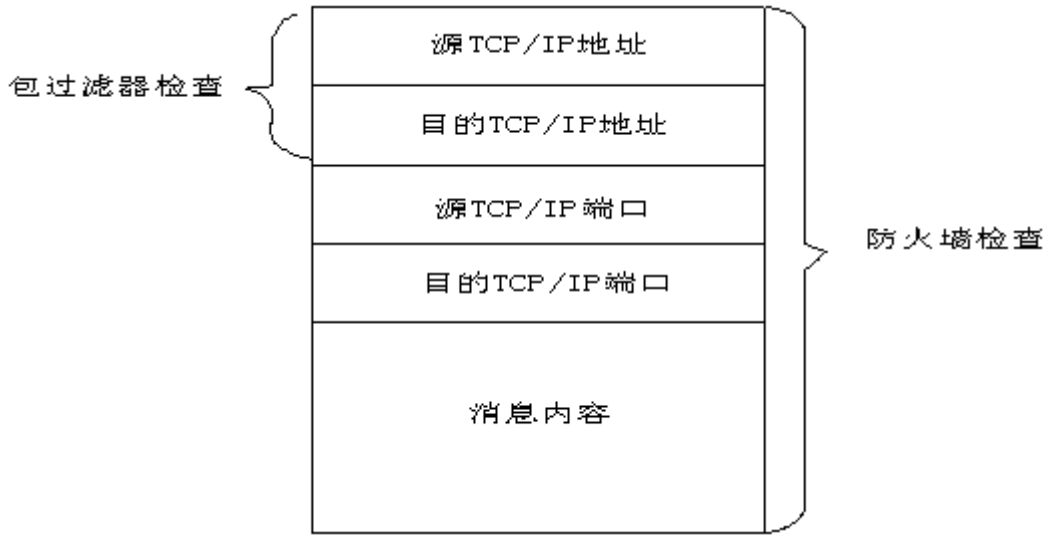


图 3 包过滤器和防火墙的信息源

端口和消息内容这些信息使防火墙比包过滤有更强的防范能力，因为这些信息使防火墙控制特定的进/出的主机地址。防火墙的功能有以下几个方面：

1、 允许或禁止特定的应用服务，例如：FTP 或 Web 页面服务；

2、允许或禁止访问基于被传递的信息内容的服务；

因为可以看到消息的内容，所以防火墙可以过滤掉令人讨厌的内容。当防火墙监测到攻击者的攻击数据包时，它可以丢弃这些包，并把该事件记录在安全日志上。

防火墙最直接的实施就是使用图 2 所示的结构，仅把局域网和 ISP 之间的包过滤器换成防火墙就可以了。这是一个防火墙的最安全的应用，因为它保护了防火墙后的所有的计算机。

但图 2 所示的安全结构存在着一个问题，它上面没有设置公共的可访问的服务器的最佳位置。你肯定不想把服务器置于防火墙的前面，在那里它将不被防火墙保护。同样，你肯定也不想把它置于防火墙后面，这样你的防火墙要允许对服务器的访问，可能会出现漏洞。

如果我们把图 2 改为图 4 所示的结构，就可以很好的解决这个问题。图 4 的结构中有 3 个端口。第三个端口连接的是另一个局域网，通常叫做 DMZ（非军事区）。DMZ 中的计算机与安全局域网中的计算机相比安全性要差一些，但是这些计算机可以接受来自 Internet 的访问。你可以把 WEB 和 FTP 服务器放在 DMZ，从而可以保护其它的计算机。防火墙上的规则设定为阻止进入安全局域网的通信数据，仅允许传出连接的建立。

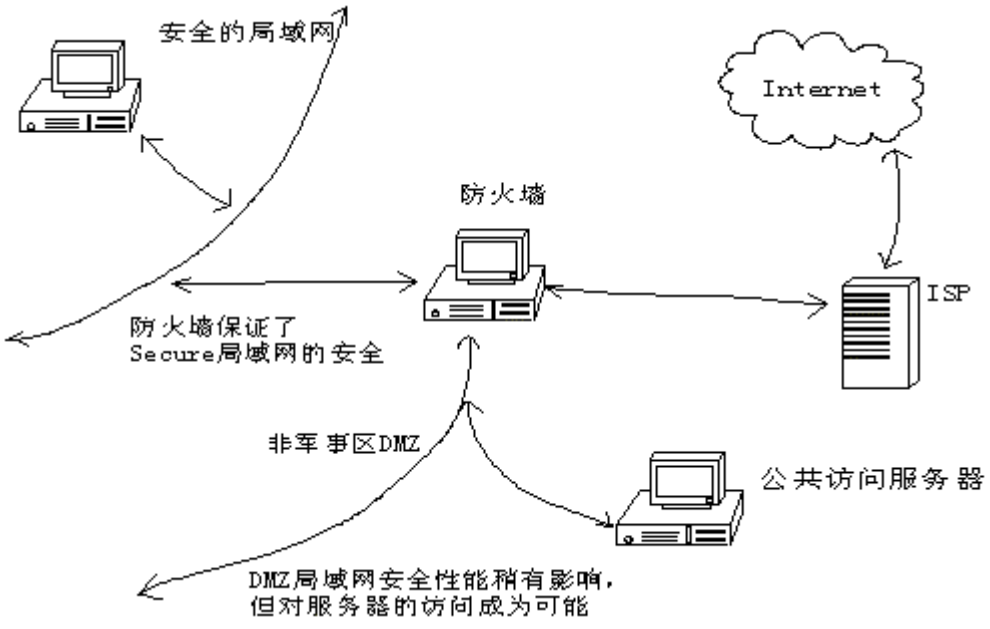


图 4 防火墙中使用 DMZ

如果你想增强 DMZ 局域网的安全性，你可以使用过滤器，限制局域网中服务器使用的端口，禁止那些来自攻击站点的访问。

为了安全你还可以给你的局域网分段，每段设置一个防火墙，每个防火墙使用不同的安全规则。需要记住的一点是，防火墙本身并没有保障安全的能力，你需要定期的检查防火墙对可疑事件做出的日志记录，你还需要去发现和使用软件的安全补丁。

如果你使用 windows98 第二版的 internet 共享连接功能，让你的一台计算机通过 MODEM 把局域网连接上 internet。在这种情况下，你的网络示很不安全的，你仍需要改善你网络的安全性。最大的威胁就是你的电脑直接连接在了 INTERNET 上，你应该直接在这台电脑上安

装包过滤器或防火器墙产品，或让你的 ISP 安装包过滤器或防火墙来保护你的访问。

请“大师”优化爱机安全

Windows9X 堪称世界上最不安全的操作系统，在默认设置下，任何人都可以在你的机器上查看文档、修改设置、安装软件，甚至用黑客软件偷窃你的密码。凡此种种，让"瘟酒吧"的用户们提心吊胆，却又无可奈何。毕竟,Windows 虽然是最不安全的系统，但也是使用最简便的操作系统之一啊！

在这里笔者为大家请来一位“大师”。它同时适用于 Windows98/Me/2000 操作系统平台，能够为你的系统提供全面、有效、简便的优化、维护和清理手段，让电脑系统始终保持在最佳状态。这就是《Windows 优化大师》，一款优秀的国产软件。当然对于我们来说，聘请它的最大的用处，还是在优化 Windows 的安全设置上。

《Windows 优化大师》在安全设置上主要针对二个方面的需求。第一方面是对木马程序、应用软件、系统端口漏洞、蠕虫病毒、普通病毒的防范；第二方面是限制他人使用本机的权力并阻止非法用户进入、修改、破坏自己的计算机系统。根据个人用户对计算机安全的两大需求。《Windows 优化大师》对此做了相当的努力，不但功能十分强大，而且使用也非常简单。在本文中笔者主要讲述《Windows 优化大师》对木马程序、系统端口漏洞、蠕虫病毒的防范方法。

下面，就让笔者为大家讲讲如何使用这些功能吧。

一、检查和免疫

《Windows 优化大师》可以检查出常见的黑客程序和病毒，并且针对一些系统安全漏洞进行修改和弥补。目前，《Windows 优化大师》能够扫描数百种黑客木马和蠕虫病毒，并且能够查找的黑客木马病毒数据还在不断增加中。要使用该功能，你需要将“扫描动作选择”框下面的三种动作方式全部勾选上。

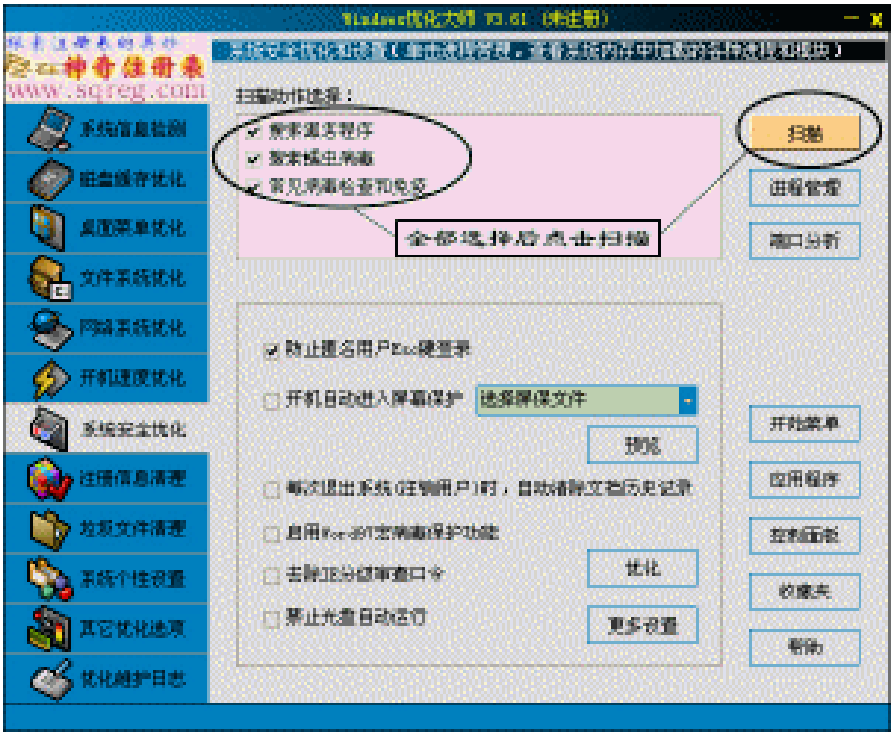


图 1

单击“扫描”，《Windows 优化大师》开始自动搜索黑客程序（通过分析可疑注册表入口、可疑文件、检查共享文件夹等方式），自动搜索蠕虫病毒、常见病毒等。与此同时，《Windows 优化大师》还能自动修补某些流行应用程序的安全性漏洞，例如 OICQ 和 ICQ 的漏洞。

《Windows 优化大师》会自动对某些蠕虫病毒进行系统免疫工作，比如笔者在搜索时发现没有对 Happy99 蠕虫病毒进行免疫，《Windows 优化大师》立刻自动补救。

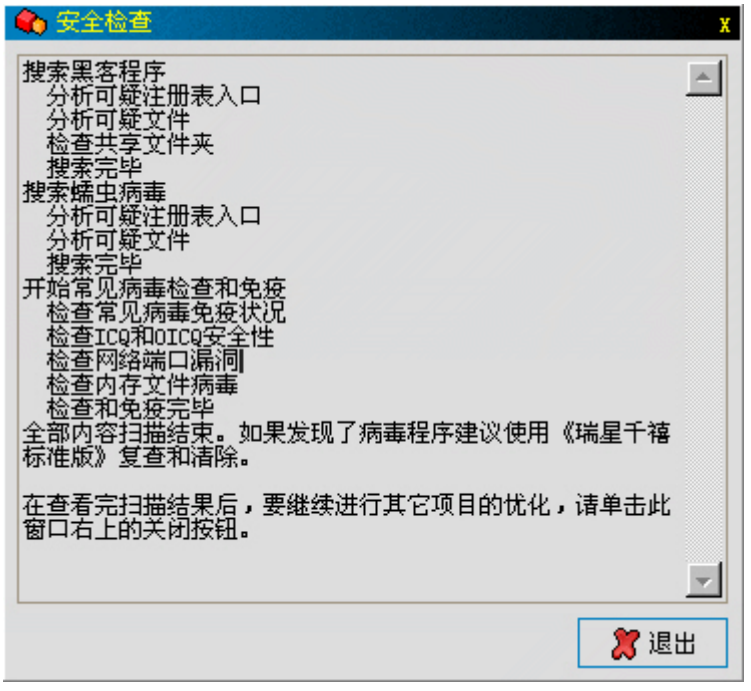


图 2

Windows 常见的端口漏洞——139 端口漏洞是黑客常见的入侵渠道。《Windows 优化大师》会自动检查网络端口漏洞并修补。所有的这些操作都是自动完成的，用户只需按下“扫描”键就能万事 OK 了。国产软件做到这个地步，真可谓精品了。

二、进程管理

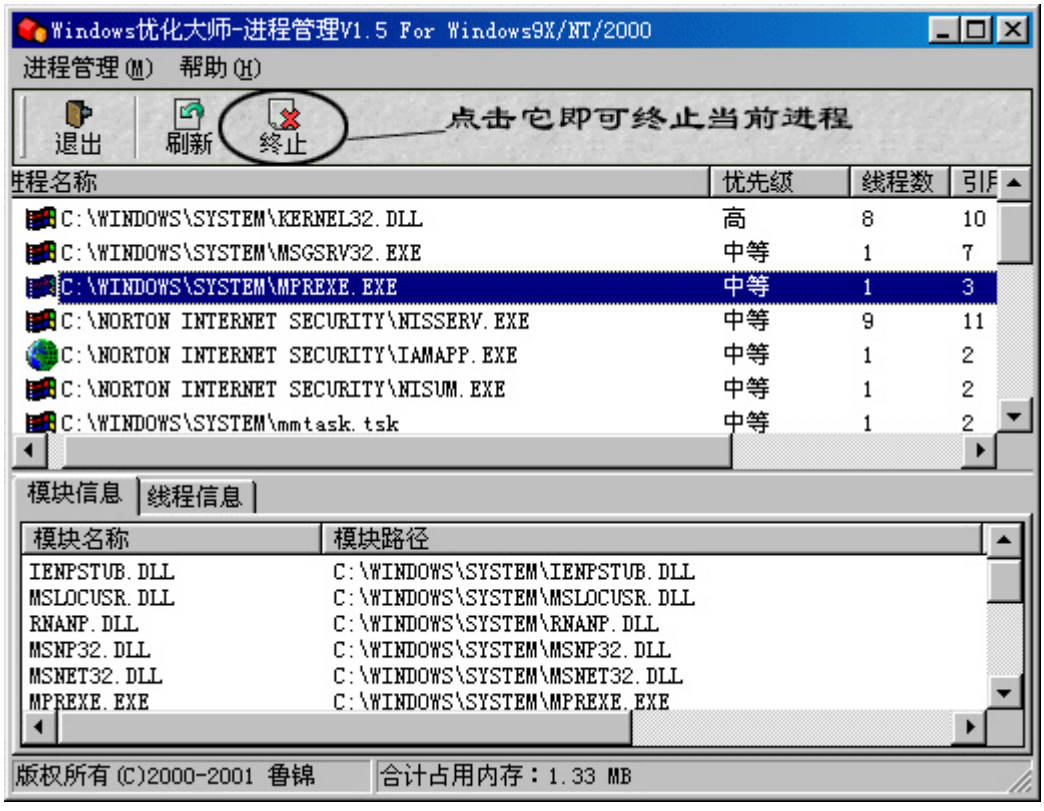


图 3

用过 Windows2000 的读者都很喜欢那个进程管理器吧，不管是木马，还是占用资源太大的程序或进程，都可以轻松杀掉。在 Win98 系统上，我们虽然可以通过查看“系统信息”中的“正在运行的任务”来查看，但是却不能对它们做些什么。使用《Windows 优化大师》的进程管理功能，计算机上正在运行的所有进程都一览无遗。我们也可以随时终止它们。注意，某些系统进程被终止会产生不可测的后果，所以要有把握的时候再做啊。

三、本地端口分析

单击端口分析就进入“本地端口分析”窗体。该窗体一共有两个标签：本地端口列表和黑客端口编辑。在“本地端口列表”单击一下“刷新”，

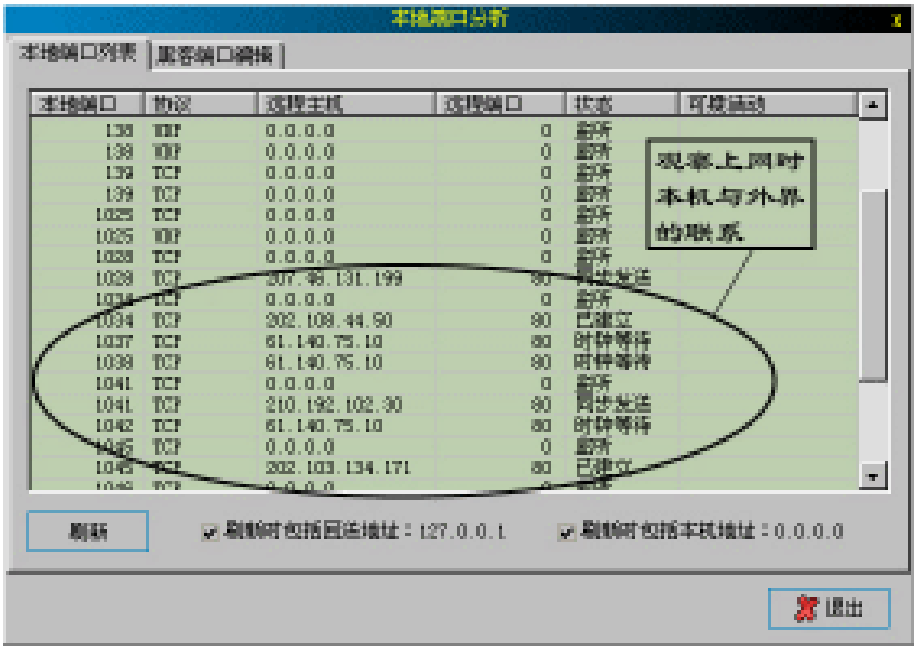


图 4

是不是看到了很多好冬冬？本机上所有打开的端口和与外界通讯的状态都一览无遗。137～139 端口是 Windows 系统上默认打开的端口，有它们才能使用 NETBIOS 协议。不幸的是，无数微软系统的入侵案件都是由 NETBIOS 协议漏洞引起的。所以我们应该看看这几个端口的连接。要是发现有外面的 IP 试图连接你的 137～139 端口，那你就要小心一点了。不过有了对方的 IP 地址，你也可以来个反跟踪对不对？

“黑客端口编辑”标签向有经验的用户提供了端口分析文件编辑功能，这样我们就能够指定某些特定的端

口来监视。比如冰河、BO2000 的默认连接端口等。这样做的好处就是一旦指定监视的端口被建立连接（通常情况下，这些端口都是不被使用的），这些可疑活动就会醒目地显示在“本地端口分析”的列表上。编写端口分析的格式十分简单。我们可以直接在“黑客端口编辑”列表最后面加上符合格式的描述就可以了。格式为：协议 端口号＝名称描述 ，例如描述 YAI 蠕虫病毒，就写上“TCP1024=NetSpy.698(YAI)”。

这样，木马之类的黑客软件再也无处隐藏了。

图 5

另外《Windows 优化大师》还有其他一些保护本机的方法，如防止匿名用户 ESC 键登录、屏幕保护设置、禁止光盘自动运行等等，我们在 这里就不再详细说了，自己去下一个试试吧!