网络安全

安全工具（一）

狄登峰 主编

目　录

千兆应用入侵防护系统—AIP

一、前言

随着对网络安全问题的理解日益深入，入侵检测技术得到了迅速的发展，应用防护的概念逐渐被人们所接受，并应用到入侵检测产品中。而在千兆环境中，如何解决应用防护和千兆高速网络环境中数据包线速处理之间的矛盾，成为网络安全技术发展一个新的挑战。

二、入侵检测技术的演进

入侵检测系统（IDS,IntrusionDetectionSystem）是近十多年发展起来的新一代安全防范技术，它通过对计算机网络或系统中的若干关键点收集信息并对其进行分析，从中发现是否有违反安全策略的行为和被攻击的迹象。IDS 产品被认为是在防火墙之后的第二道安全防线在攻击检测、安全审计和监控等方面都发挥了重要的作用。

但在入侵检测产品的使用过程中，暴露出了诸多的问题。特别是误报、漏报和对攻击行为缺乏实时响应等问题比较突出，并且严重影响了产品发挥实际的作用。Gartner 在 2003 年一份研究报告中称入侵检测系统已经“死”了。Gartner 认为 IDS 不能给网络带来附加的安全，反而会增加管理员的困扰，建议用户使用入侵防御系统（IPS,IntrusionPreventionSystem）来代替 IDS。Gartner 公司认为只有在线的或基于主机的攻击阻止（实时拦截）才是最有效的入侵防御系统。

从功能上来看，IDS 是一种并联在网络上的设备，

它只能被动地检测网络遭到了何种攻击，它的阻断攻击能力非常有限，一般只能通过发送 TCPreset 包或联动防火墙来阻止攻击。而 IPS 则是一种主动的、积极的入侵防范、阻止系统，它部署在网络的进出口处，当它检测到攻击企图后，它会自动地将攻击包丢掉或采取措施将攻击源阻断。因此，从实用效果上来看，和 IDS 相比入侵防御系统 IPS 向前发展了一步，能够对网络起到较好的实时防护作用。

近年来，网络攻击的发展趋势是逐渐转向高层应用。根据 Gartner 的分析，目前对网络的攻击有 70％以上是集中在应用层，并且这一数字呈上升趋势。应用层的攻击有可能会造成非常严重的后果，比如用户帐号丢失和公司机密泄漏等。因此，对具体应用的有效保护就显得越发重要。从检测方法上看，IPS 与 IDS 都是基于模式匹配、协议分析以及异常流量统计等技术。这些检测技术的特点是主要针对已知的攻击类型，进行基于攻击特征串的匹配。但对于应用层的攻击，通常是利用特定的应用程序的漏洞，无论是 IDS 还是 IPS 都无法通过现有的检测技术进行防范。

为了解决日益突出的应用层防护问题，继入侵防御系统 IPS 之后，应用入侵防护系统（AIP,ApplicationIntrusionPrevention）逐渐成为一个新的热点，并且正得到日益广泛的应用。

三、应用入侵防护

对应用层的防范通常比内网防范难度要更大，因为这些应用要允许外部的访问。防火墙的访问控制策略中必须开放应用服务对应的端口，如 web 的 80 端口。这样，黑客通过这些端口发起攻击时防火墙无法进行识别

控制。入侵检测和入侵防御系统并不是针对应用协议进行设计，所以同样无法检测对相应协议漏洞的攻击。而应用入侵防护系统则能够弥补防火墙和入侵检测系统的不足，对特定应用进行有效保护。

所谓应用入侵防护系统 AIP，是用来保护特定应用服务（如 web 和数据库等应用）的网络设备，通常部署在应用服务器之前，通过 AIP 系统安全策略的控制来防止基于应用协议漏洞和设计缺陷的恶意攻击。

在对应用层的攻击中，大部分时通过 HTTP 协议（80 端口）进行。在国外权威机构的一次网络安全评估过程中发现，97％的 web 站点存在一定应用协议问题。虽然这些站点通过部署防火墙在网络层以下进行了很好的防范，但其应用层的漏洞仍可被利用进而受到入侵和攻击。因此对于 web 等应用协议，应用入侵防护系统 AIP 应用比较广泛。通过制订合理的安全策略，AIP 能够对以下类型的 web 攻击进行有效防范：

恶意脚本

Cookie 投毒

隐藏域修改

缓存溢出

参数篡改

强制浏览

Sql 插入

已知漏洞攻击

应用入侵防护技术近两年刚刚出现，但发展迅速。YankeeGroup 预测在未来的五年里，AIP 将和防火墙，入侵检测和反病毒等安全技术一起，成为网络安全整体解决方案的一个重要组成部分。

四、千兆解决方案

应用入侵防护产品在保护企业业务流程和相关数据方面发挥着日益重要的作用，同时随着网络带宽的不断增加，只有在适合千兆环境应用的高性能产品才能够满足大型网络的需要。

传统的软件形式的应用入侵防护产品受性能的限制，只能应用在中小型网络中；基于 x86 架构的硬件产品无法达到千兆流量的要求；近年来，网络处理器（NP）在千兆环境中得到了日益广泛的应用，但 NP 的优势主要在于网络层以下的包处理上，若进行内容处理则会导致性能的下降。

通过高性能内容处理芯片和网络处理芯片相结合形式，为千兆应用入侵防护产品提供了由于的解决方案。其设计特点是采用不同的处理器实现各自独立的功能，由网络处理芯片实现网络层和传输层以下的协议栈处理，通过高速内容处理芯片进行应用层的协议分析和内容检查。从而实现了千兆流量线速转发和高速内容处理的完美结合，真正能够为用户提供千兆高性能的应用防护解决方案。

在上面系统框架中，包处理引擎收到数据包后，首先由网络处理器进行传输层以下的协议栈处理，并将数据包还原成数据流。接下来由内容处理器对数据流进行应用协议处理，根据控制器设定的安全策略对各种应用攻击进行检测和过滤。只有符合安全策略要求的数据流才会被发送到服务器，攻击包则被丢弃。

在高性能的千兆解决方案中，能够实现网络层到应用层的多层次立体防护体系。对于面向大型 web 应用，产品通过多种功能的集成实现有效的应用防护：

Web 应用入侵防护。通过系统内置的网络内容处理芯片，对 web 请求和回应流量进行细致的分析。根据内置的规则及启发式的安全策略，有效防范各种针对 web 应用的攻击行为。

DOS 攻击的防护。系统通过网络处理芯片，对 Synflood、Icmpflood、Upflood、PinfOfDeath、Smurf、Ping Sweep 等网络层的拒绝服务攻击进行过滤的防范，有效保护服务器。

访问控制。通过硬件的 ACL 匹配算法，系统能够在实现线速转发的同时对数据包进行实时的访问控制。

中科网威在新一代千兆应用入侵防护产品设计中采用了上述解决方案，实现了千兆流量下的线速处理。系统以透明模式接入网络，在增强安全性的同时，网络性能不会受到任何影响，真正实现了应用层内容处理和千兆高性能的完美结合。

五、小结

为了保护企业重要的应用服务资源，应用入侵防护产品 AIP 正在得到日益广泛的应用。中科网威通过内容处理器和网络处理器相结合的技术，有效解决了千兆网络环境中应用入侵防护和性能之间的矛盾，为用户提供了全新的解决方案。

用 ISA+瑞星构筑网络安全的铜墙铁壁

前序

随着当今信息社会的迅猛发展，信息化浪潮已遍布各行各业。同时由于电子商务和电子政务的推行，使得

社会信息化发展得更快，因此这就需要各个单位进快汇入信息化的大潮中，否则就有可能被社会所淘汰。然而就在企业连上互联网的那一刻开始，网络安全的问题就摆在了各个单位面前。那么我们怎样才能既安全又高效的连上互联网上呢？或许安装 ISA+瑞星网络版杀毒软件是一个不错的办法，下面我将结合我单位网络建设中怎样利用 ISA+瑞星网络版杀毒软件来构筑安全网络的事例来阐述其构成。

关键词

ISA 瑞星网络版杀毒软件网络安全防火墙代理服务

正文

一、为什么要用 ISA+瑞星网络版杀毒软件来构造安全网络

自从网络用户连上互联网的那一刻开始，网络安全问题就放在了我们面前。如果不做好网络安全防卫工作，那么就可能造成网络内部数据被盗或丢失、网络瘫痪、病毒泛滥等，这样就使得网络用户不能正常工作。

安全问题是每个单位都不敢掉以轻心的，只要任何一个单位在网络上存在，那么必须对自己进行保护，免受恶意和敌意的入侵与攻击的伤害。伴随着 Internet 的成长，黑客和黑客工具无论在数量还是质量上都逐渐发展状大。为了解决这个问题，市面上的防火墙产品也呈爆炸性增长趋势。但所有软件各有千秋，其功能和价格也不一样，因此就其实用性来说，我们选择了 ISA，因为它不但具有防火墙的功能，而且更主要的是有代理和高速缓存的功能。同时它还可以按照用户的要求量身定做的开放相应的协议和端口，因而网络安全就更胜一筹。同时由于瑞星杀毒软件的强大防毒和杀毒功能，以及瑞

星的时时在线升级功能，使得瑞星在杀毒方面技胜一筹，因此我们就选用了 ISA+瑞星网络版杀毒软件来构造安全网络。

二、ISA 的安装与配置

1、ISA 的安装

当我们买回 ISA 软件后，首先应该阅读一下软件安装说明，这对我们正确安装软件百利而无一弊。同时要特别注意 ISA 标准版和企业版的异同之处。ISA 标准版需要安装到一台独立的 Windows2000 服务器上，而且只能使用本地安全策略，它不需要 ActiveDirectory 的支持。而企业版必需要 ActiveDirectory 的支持，它同 ActiveDirectory 紧密地集成在一起，它还利用 ActiveDirectory 保存配置和策略信息。由于我们单位的网络是一个中型网络，所以我们用不着去买 ISA 企业版（因为企业版要比标准版贵很多），因此我们最后选用了 ISA 标准版。

在安装 ISA 之前，首先要安装好 Server2000 操作系统，且保证所装区域为 NTFS 格式。在装好系统后，必须要确保所装服务器上有两块网卡，并且两块网卡都设置好，一块网卡配置外部 IP 地址，另一块网卡配置内部 IP 地址。同时要配置好两块网卡的各自网关和 DNS 地址。要注意的是内部网卡的网关地址请不要填写。同时去掉操作系统中的 IIS 和其它不相关的程序，只保留一个纯 Server2000 操作系统。在做好这些基础工作之后，就可以将 ADSL 专线（我单位申请的是 ADSL 专线）插在外部网卡上，同时在服务器上测试线路的连通信，以确保服务器现在能连上互联网。否则得重新检查硬件和软件的安装，以确保服务器必须能连上互联网。在做好这些基本工作后就可以安装 ISA 软件了。

当我们把 ISA 光盘放入光驱之后，它会自动弹出一个界面让用户去选择。首先它须确保操作系统能满足它的安装要求。否则用户就得更新系统，以符合安装要求。ISAServer 有三种安装模式：防火墙模式、高速缓存模式、综合模式。在综合模式下，防火墙和缓存功能会被整合到一起，以便同时利用网络安全和 Web 缓存方面的功能。因此我们选用了综合模式。

在安装期间配置 LAT 时，必须注意要根据内部网络实际使用的地址来配置，必须要配置正确，否则就不能正常运行。这可根据主控服务器的设置来进行配置。例如我单位在装主控服务器时就设定了内部网络地址为：192.168.0.0～192.168.0.255，因此我们在 LAT 中就填入该内部 IP 地址。在设置 Web 缓存时，最好能选择剩余区间最大且不与程序文件同一个分区的磁盘分区，其缓存文件大小可根据实际情况来决定，但其大小最好能大一些，我单位就配置了一个 1G 大小的 Web 缓存文件。

2、ISA 协议的配置

在装好程序文件后，就得配置相应的访问规则，这样内部用户才能访问英特网。其中最主要的是访问 Web 协议和访问邮件服务协议，其它象访问 FTP、QQ、Net Meeting、证券之星等程序的协议可根据实际情况来决定是否开放。

访问 Web 协议的开放可以通过以下来完成：在 ISA Management 中，展开计算机，找到 AccessPolicy/ProtocolRules/CreateaProtocolRuleforinternetAccess，点击它，一路按默认值进行配置，即 Protocol 中有 FTP、FTPDownloadonly、Gopher、Http、Https，Action 为 Allow，Schedule 为 always、Appliesto 为 AnyRequest。

要访问邮件服务器上的邮件就得开放与 DNS 相关的协议，如 DNSQuery、DNSQueryServer、DnsZoneTransfer、DnsZoneTransferServer 四个协议。

3、WEB 服务器和邮件服务器的发布

要进行 WEB 发布，可按以下步骤进行：在 ISAManagement 控制台中，展开计算机名，找到 PolicyElements/DestinationSets/CreateaDestinationSet，点击它，在 name 中输入所添加目标的名字，最好输好记的名字，如域名等。然后在 includethesedestinations/add/Destination 中输入单位网站网址。然后就 OK 了。接着找到 Publishing 节点。右击 WebPublishingRules 节点，点击 New，然后选 Rule。在向导的第一页输入该规则的名字，可命名为 ExeterWeb，点 Next；在目标集合页中，在 Applythisruleto 下拉框中选择 Specifieddestinationset，在 Name 下拉框中选择我们前面已经建立好的目标的名字，例如前面建设好的域名，点击 Next。在 ClientType 中选择 Any Reqest。因为我们开放网站的目的就是要让外界所有人看，所以就选择此项，再点击 Next，在 RuleAction 中可以根据不同的情况选用不同的方式，我们选用了第二种方式 Redirecttherequesttothisinternalwebserver(nameorIP address)，在其中最好能输入网站服务器的 IP 地址。因为我单位网站放在内部，其 IP 为 192.168.0.3，所以我们就将其输上。同时我们应在下面的 sendtheoriginalhostheadertothepublishingserverinsteadoftheactualone(specifiedabove)前面的方框内画上勾，其下面各小项的值最好不要改动，使用其默认值。最后一页可以看一下所有配置，如果正确就点击 Finish 就完成了网站的发布。

邮件服务器的发布可通过以下步骤来进行：在 ISA

Management 中，展开 Publishing 节点，右击 ServerPublishingRules 节点，点击 SecureMailServer。在对话框中，选中 DefaultAuthentication 和 SSLAuthentication 中的所有选项，然后点击 Next，在 ISAServer′ sExternalIPaddressd 页中，输入 ISA 所在服务器的外部接口的 IP 地址，即互联网上的 IP 地址，然后点击 Next。在 InternalMail Server 页中选择 AtthisIPaddress，在其中输入内部邮件服务器的 IP 地址（192.168.0.1），然后点击 Next。在向导的最后一页，如果我们确认所有设置无误后就可以点击 Finish 以完成配置，系统自动创建许多新的服务器发布规则。这样邮件服务器就发布完成。

4、客户端的安装

ISAServer 客户机类型有三种：SecureNAT、防火墙客户机、Web 代理客户机。但为了能充分利用 ISA 本身所具有防火墙功能，我们选用了防火墙客户机来安装客户端。客户端的安装路径为：\\ISA 服务器名\mspclnt\setup.exe。

三、瑞星网络版杀毒软件的安装

瑞星网络版杀毒软件的控制中心最好能安装在 ISA 服务器即网关上。因为这样做就可以将病毒控制在外网中，以致于将病毒完全隔离在外网，不会向内网传播。在安装过程中，要注意系统控制中心的 IP 地址一定要设置成外部 IP 地址，此点切记。

在安装好系统控制中心后，接着按照提示安装好服务器端和客户端。在服务器端的升级设置中，如果是专线的话，最好设置成在某一固定时间自动下载升级，这样即保证了病毒库的时时更新，又不必需要网络管理员天天去手动下载升级。

要注意的是，如果邮件服务器安装在内网中，并且是用 ExchangeServer2000 来作为邮件服务器，同时没有买瑞星专门针对 ExchangeServer2000 设置的程序的话，就得注意必须关掉网关（ISA 服务器）和邮件服务器上的邮件监控，即关闭邮件发送监控和关闭邮件接收监控。只有这样，才能保证 ExchangeServer2000 邮件服务器正常运行和客户端正常收发邮件。

在安装好所有客户端后，要定期地在服务器上对整个网络的所有计算机进行联网杀毒，彻底杀灭内部的一些原来没有被杀的病毒，以保证整个网络的安全。

结束语

通过 ISA+瑞星网络版杀毒软件在网络上的配置，就使得整个网络的安全大大提高，从而维护了整个网络在互联网上的安全性，这对黑客的攻击和病毒泛滥可以构筑起一堵铜墙铁壁来保证网络的安全与正常运行。

了解自己电脑的“安全红线”

所谓安全红线，就是你机器的安全底线，我想这就不必我过多的解释了。但是大家在一般测试时都开这防火墙和杀毒软件测试，这其实也没有什么不妥的。但是此时测试的是你在有防御能力下的情况，并无法知道你真正的“安全红线”而且对于 100%克隆体来说防火墙和杀毒软件并不具有独特性这也就意味着它是可以突破的！况且如何绕过杀毒软件和防火墙应该是黑客的最基本技术……

那如何了解自己的安全红线哪？向你推荐你一个微

软的免费小工具 MicrosoftBaselineSecurityAnalyzer(系统安全分析及解决工具)它可以测试你个人计算机及指定 IP 机器的安全情况重点安全隐患将以红色的“X”表示，并向你提供解决方案。

其实向你推荐这款工具没有别的意思，就是让你摧毁自己原有的安全自信！

1、你以为自己安装所有补丁就很安全了吗？那你使用的 FAT32 分区就是一个安全隐患，毕竟微软新系统的安全及稳定性都是建立在 NTFS 分区基础之上，虽然每一个用户都有使用 FAT32 的理由，但是要知道微软的新版 LONGHORN 系统仅仅支持 NTFS。如果你还不想放弃微软的话我强烈建议你使用 NTFS 至少也在系统分区使用！况且你也需要一段时间适应 NTFS 比如你如果想在 DOS 删除 NTFS 分区哪对你将是一场噩梦！

2、安全与性能之间的平衡。现在很多用户已经越来越的使用“管理”和“本地安全策略”等设置来完善自己的安全性能，这绝对是是意味这你安全意识已经进行一次飞跃。而且你计算机的安全性能也绝对会有极大的加强，但是这也不是没有任何代价的！因为这些都是通过设置关闭系统一些“不长用”的功能，或开启系统某些安全设置达到目的。但是在我目前接触到的网上/印刷资料中还没有哪一个能详尽完全对此进行说明。比如某些文章说某项服务“不常用”普通用户可以禁止，但是“不长用”并不等于没有用，什么是普通用户？用户在什么情况下开启什么情况下关闭作者就避而不谈了，但是对于用户来说此时你的系统就成了“女孩的心思”你将会不断碰到莫名其妙的问题。

打个比方，这样的设置就犹如一个天平有经验的用

户可以在安全与性能之间找到平衡，但是这平衡只是一点稍不留神天平就倾向一边。

我说的“安全红线”就是让用户知道，自己系统的安全底限是什么。只有这样才能做到知己知彼，但是你别想百战不胜。用户的安全仅仅只放在安全软件+补丁+设置上，但是我要是黑客不绝对不会在这些上面跟用户叫劲，最强大的堡垒是从那里攻破的？聪明的用户会站在黑客的角度看问题，不是吗？

图解“微软网络安全热修补检查器”

对 Windows 管理员来说，坚持关注最新的安全补丁是至关重要的。为此，微软发布了“微软网络安全热修补检查器”（NetworkSecurityHotfixChecker）。这个工具允许管理员扫描 Windows 系统，确保当前所有安全补丁已经生效。

该热修补检查器是一个命令行工具，它察看在 Windows 服务器中安装的所有补丁的状况，并告诉你，它们是否是最新的。该工具通过参阅微软定期更新的公共 XML 数据库来完成这个工作。你可以使用这个工具来获知如下产品的补丁状况：

Windows2000

WindowsNT4.0

InternetInformationServices(IIS)4.0/5.0

InternetExplorer(IE)5.01+

SQLServer7.0/2000

安装并使用该工具

当你下载该工具后，系统提示你选择安装这个可执行文件的位置。选择适当的目录并运行可执行文件。如图 1 所示的是，将被放到指定目录的该工具的各个文件。

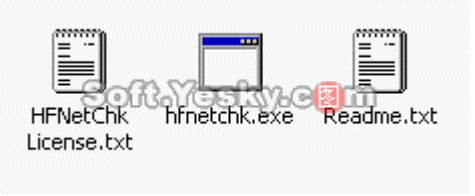

图 1

运行热修补检查器：

打开命令提示符窗口，进入热修补检查器的安装目录（如图 2）。

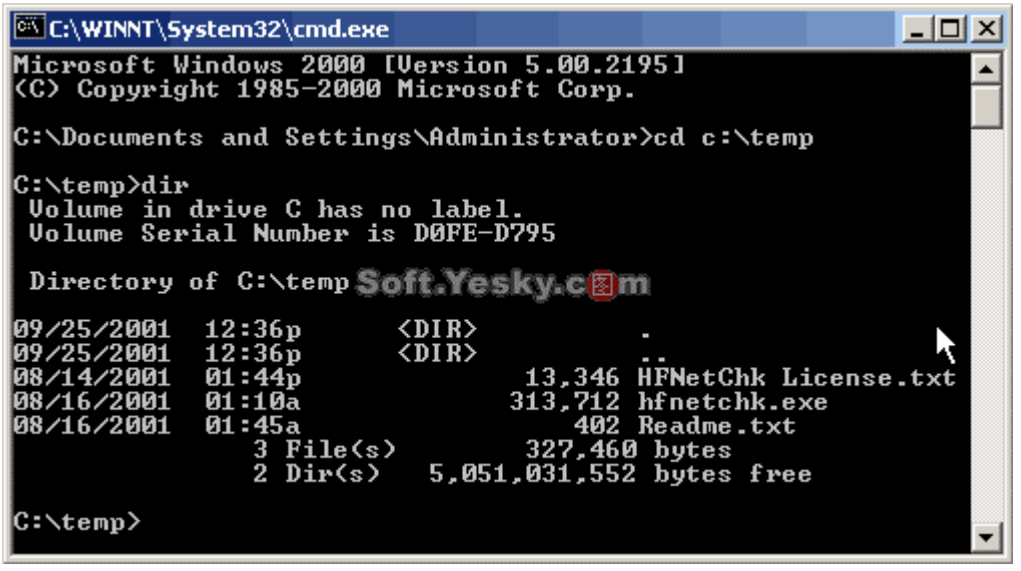

图 2

键入 hfnetchk，按回车键，你将看到如下屏幕（如图 3）。

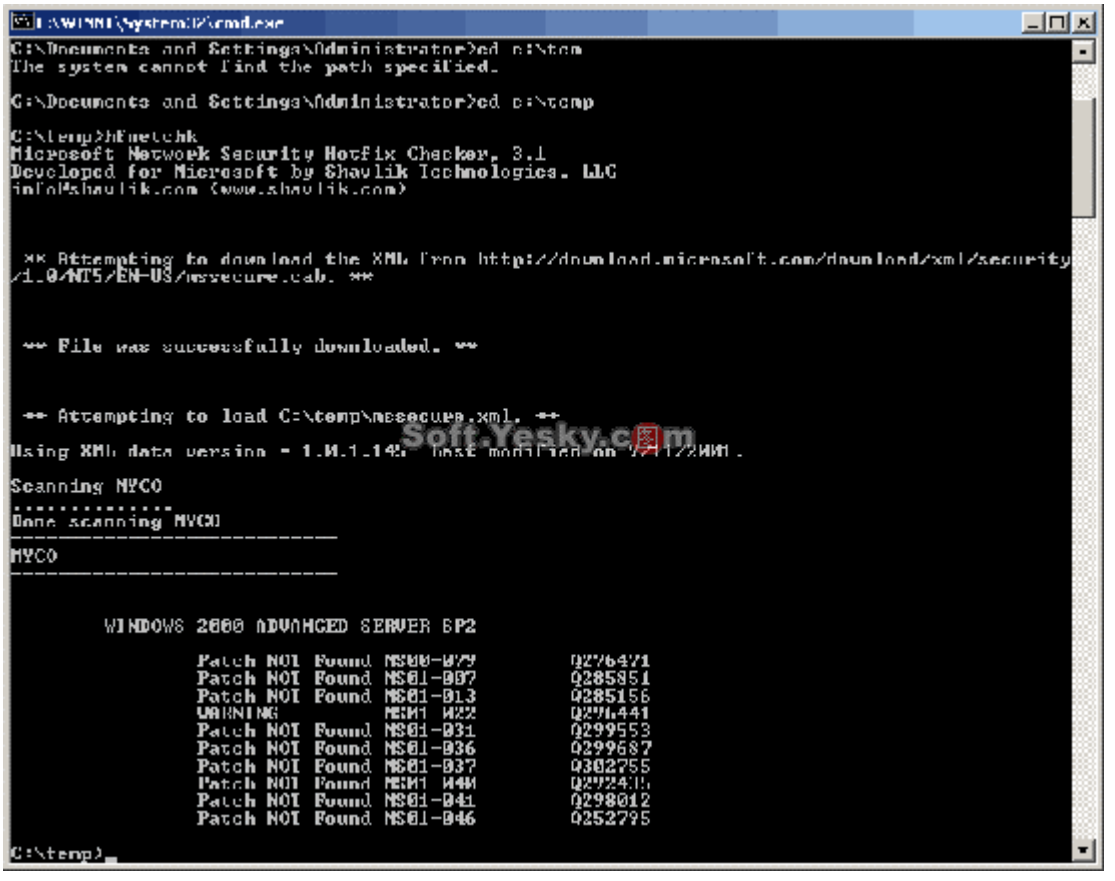

图 3

要查看更详细的解释，请键入 hfnetchk-v-z，**回车后如下图所示（如图** 4）。