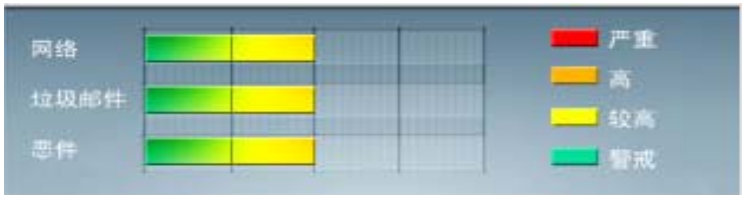
安全威胁每周警讯

2010/10/31～2010/11/07

本周威胁指数



TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	TROJ_IFRAME.CP	木马病毒	★★★	↓	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。 当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
4	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
5	Cryp_Xed-12	木马	★★★	→	疑似病毒
6	PAK_Generic.001	加壳程序	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
7	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
8	CRCK_KEYGEN	破解程序	★★	→	非法破解程序
9	JS_EXPLOIT.SMD	网页病毒	★★★	↓	该 JavaScript（JS）的恶意软件可能被托管在一个网站，当用户访问网站时运行并感染。同时，它可能是其他恶意软件的组成部分。通常它检查的 Adobe Flash Player 的系统中安装的版本。然后，它尝试下载一个 SWF 文件根据的 Flash Player 的版本安装。
10	Gray_Gen	灰色软件	★★★	→	灰色软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件

系统漏洞信息

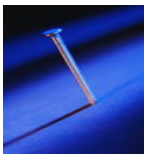
MS10-084:Windows 本地过程调用中的漏洞可能导致特权提升 (2360937)

受影响的软件:

Windows XP

Windows Server 2003

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-084.mspx



系统安全技巧

摘要: 当前，Web 服务器上面的信息越来越丰富和重要，Web 服务器的重要性也非常明显。因此就需要使用防火墙来保护它，如果要将 Web 服务器放在防火墙之内，则需要防火墙的支持。 下面我们来看看如何用反向代理技术来保护 Web 服务器。

为了增加网络的安全和保护内部网络上的重要数据，需要将内部网与 Internet 相隔离，当前主 要通过防火墙技术来完成这个目的。然而为了保护内部主机，防火墙软件就必须限制外部网络中的主机对内部网络的访问。因此普通防火墙软件的设置中，外部网络 无法访问内部主机。然而，为了向外发布自己的信息，就需要允许外部网络访问自己的 Web 服务器。最简单的处理方法是将 Web 服务器放在防火墙之外，这样就 将 Web 服务器和内部网络区分开，Web 服务器暴露在网络外部，就有可能招受攻击而导致服务器瘫痪或网页被更改等潜在的问题。而当前，Web 服务器上面的 信息越来越丰富和重要，Web 服务器的重要性也非常明显。因此就需要使用防火墙来保护它，如果要将 Web 服务器放在防火墙之内，则需要防火墙的支持。

当前防火墙主要有两种类型，一种为包过滤型防火墙，这种防火墙针对每个 IP 包识别它是否符合管理 员设定的过滤规则，符合一定要求的才被正确转发。可以使用的过滤规则包括源和目的主机的名字和 IP 地址，端口地址，使用的网络界面，以及 IP 包的类型。通常包过滤型的防火墙软件根据 IP 包的类型屏蔽所有的由外部发起的连接请求，从而保护内部网络。如果 要将 Web 服务器放在放火墙之内，就需要允许对这个 Web 服务器和它使用的 TCP 端口的访问。

另一种类型的防火墙为应用代理型的防火墙，这种防火墙针对每种应用协议提供相应的代理服务，由代 理服务器访问网络，并将结果返回给客户机。标准的 http 协议的代理服务，客户端的浏览器必须配置代理服务器的 IP 地址，不可能要求其他外部主机为访问这 个内部网络上的主机而重新设置代理服务器的地址。代理服务器并不区分外部网络和内部网络，但是代理服务器使用 Internet 上的名字解析来确定 Web 服 务器的位置，而通常防火墙内使用内部地址，这也决定了普通代理型防火墙不支持外部网络对内部 Web 服务器的 http 访问请求。因此普通代理服务器简单的屏 蔽外部地址的访问，因此最简单的保护对外发布信息的 Web 服务器的方式是使用包过滤型的防火墙。

一旦允许外部网络中的主机可以向内部网络发起连接请求，攻击者就可以在网络外部尝试进行连接，这 增加了攻击者攻击内部网络的方式，降低了整个网络的安全系数。如果不允许外部主机向内部网络发起连接请求，攻击者就只好在外部发起攻击，使用特洛伊木马或 者 IP spoof 等技术，这些方式与发起主动连接的攻击方式相比，没有现成的工具供利用，因此使得攻击的复杂性大大增加，因此网络被攻击的可能性大为减少，几乎 成为不可能。一旦攻击者进入内部网络中的 Web 服务器，整个内部网络就暴露在攻击者的面前，防火墙就不能起到应有的作用了。因此

通过重新定义包过滤型防火 墙的过滤规则，并将 Web 服务器放在内部网络内，只是一种简单的保护 Web 服务器的方法，然而不利于保护整个内部网络的安全。

因此，为了在保护 Web 服务器和内部网络的安全，当前使用的更安全的做法是实现双层防火墙。外层 防火墙实现包过滤功能，然而却允许外部网络访问其中的 Web 服务器，内部防火墙允许最中间的内部网络可以访问外部网络。在外部防火墙和内部防火墙之间称为 停火区，提供外部网络访问的服务器就位于这个区域，表明即使攻击者通过外部防火墙进入这个区域，也无法攻入内部网络。双层防火墙通过设置了两层防火墙，使 得内部网络更为安全。然而，它在保护 Web 服务器方面的作用，与单层防火墙相似。因为此时 Web 服务器仍然只受到一层防火墙的保护，同样也无法对外部隐藏 防火墙内主机的各种信息，例如服务器的 ip 等。而且这层防火墙是对应用协议一无所知的包过滤防火墙，由于包过滤的方式不识别应用协议，通常为 http 协 议，那么就无法正确识别外部的连接请求是否属于正常连接，通常也无法进行详尽的连接记录。为了更好的保护 Web 服务器不被外部攻击者破坏，就应该屏蔽内部 服务器的 IP 地址等信息，并且防火墙能够识别连接协议，显然这是代理型防火墙的任务。

通常的代理服务器，只用于代理内部网络对 Internet 的连接请求，客户机必须指定代理服务 器，并将本来要直接发送到 Web 服务器上的 http 请求发送到代理服务器中。由于外部网络上的主机并不会配置并使用这个代理服务器，普通代理服务器也被设计为在 Internet 上 搜寻多个不确定的服务器,而不是针对 Internet 上多个客户机的请求访问某一个固定的服务器，因此普通的 Web 代理服务器不支持外部对内部网络的访问 请求。当一个代理服务器能够代理外部网络上的主机，访问内部网络时，这种代理服务的方式称为反向代理服务。此时代理服务器对外就表现为一个 Web 服务器， 外部网络就可以简单把它当作一个标准的 Web 服务器而不需要特定的配置。不同之处在于，这个服务器没有保存任何网页的真实数据，所有的静态网页或者 CGI 程序，都保存在内部的 Web 服务器上。因此对反向代理服务器的攻击并不会使得网页信息遭到破坏，这样就增强了 Web 服务器的安全性。

反向代理方式和包过滤方式或普通代理方式并无冲突，因此可以在防火墙设备中同时使用这两种方式， 其中反向代理用于外部网络访问内部网络时使用，正向代理或包过滤方式用于拒绝其他外部访问方式并提供内部网络对外部网络的访问能力。因此可以结合这些方式 提供最佳的安全访问方式。

综合反向代理功能和普通拒绝外部访问的普通防火墙软件相结合，就能构成一个既具有保护内部网络、 又能对外提供 Web 信息发布的能力的防火墙系统。由于反向代理能力需要软件实现，因此不能使用现有的防火墙系统，需要使用相关软件进行开发改进。Unix 显然是首选平台，我们基于 FreeBSD 系统，提出一种基于 ipfw、natd 与 squid 的防火墙设置方式。其中 ipfw 可以基于 ip 地址、端口、协议等对 ip 包进行过滤，natd 提供网络地址转换功能，这样就隐藏了内部网络的拓扑 等信息，ipfw 和 natd 结合就构成了强大的包过滤网关。而 squid 是 Internet 上最流行的 Web 代理服务器之一，虽然它提供的是普通的正向代 理能力，但其为开放源代码软件，并且具有强大的可配置性，因此很容易可以将其更改为反向代理服务器。

这种方式对内部网络的保护能力，要小于双层防火墙软件，等于普通的单层防火墙软件，然而其对 Web 服务器的保护却大于双层防火墙系统中对位于对停火区内的 Web 服务器的保护。然而其本身为单层系统，因此比双层系统配置起来更方便，是一种简单有效 的方案。其中反向代理功能能够提供丰富的连接记录，可以用来提供预防和捕获攻击的能力，而包过滤和网络地址翻译可以让内部网络的主机可以使用多种协议访问 外部网络，不需要考虑防火墙对应用协议的支持问题。这种方式适用于大多数 Intranet 系统。

当需要对内部网络提供更进一步的保护时，仍然可以使用双层防火墙模式，这样兼具反向代理对 Web 服务器的保护能力，和双层防火墙对内部数据的更大的保护能力。

当组织向外提供信息发布的时候,并不仅仅要提供一些静态的网页,更大的可能是要根据实际的数据动 态发布信息。因此发布的网页便需要通过访问数据库动态生成,通常使用的动态生成技术有 CGI 或服务器端文档解析等方式生成

的。然而无论那种方式，都需要使 得 Web 服务器能够和数据库服务器进行连接、通信。然而系统数据库应该是内部网络中应该首要保护的系统，因此要求安全性要求不高的对外发布信息的 Web 服 务器和内部数据库服务器放置在同一个网段，就会造成相应的安全问题。

为了提高访问数据库服务器的安全性，就需要对能够访问数据库的 CGI 程序进行限制，这就要求对启 动 CGI 的 URL 请求比对普通 url 进行更严格的限制。与普通包过滤型防火墙不同，反向代理能够理解 http 协议，能区分出不同的 url 请求，从而能够实现对 cgi 请求比普通 http 请求更严格的控制，甚至可以将 cgi 请求发送到一台专用的 CGI 服务器进行处理，从而分别处理普通 url 请求和 cgi 请求。这台 cgi 服务器可以具有访问 数据库的能力，保证数据库的安全。

总结本文中的论述，可以看出，反向代理方式是一种对外提供 Web 发布时使用的有效的防火墙技术，使用它和传统防火墙技术相结合，就能实现简单有效的防火墙系统。

来源： XKER