文章编号:1005－0523(2005)04－0065－03

构建安全 web 服务器探析

章海亮

(华东交通大学 机电工程学院,江西 南昌 330013)

摘要:描述了计算机网络安全容易受到黑客的威胁和攻击。论述了用 IIS4.0 构建安全 Web 服务器的方法,对在设置过程中产生的有关问题进行了较好的解决.

关 键 词:计算机网络;安全;IIS4.0

中图分类号:TP393.08 **文献标识码**:A

影响计算机网络安全的因素很多,这些因素可能是有意的,也可能是无意的;可能是人为的,也可能是非人为的;可能是外来“黑客”(Hacker)对网络系统的攻击,也可能是系统内部的合法用户对系统资源的非法使用,归结起来,针对网络安全的威胁主要有以下几点:

1) 人为的无意失误:如操作员安全配置不当造成安全的漏洞,用户安全意识不强,用户口令选择不谨慎,用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁.

2) 人为的恶意攻击:恶意非法进攻是现在面临的最为严重的问题.“黑客”(Hacker)通过各种非法途径进入内部网络,复制、修改、甚至销毁机密信息,造成极大危害.

3) 网络软件的漏洞和“后门”:网络软件不会百分之百的无缺陷和无漏洞的,这些漏洞恰恰是黑客进行攻击的首先目标,一旦“后门”洞开,所造成的危害不堪设想.

为了应对网络面临的危险和攻击,需要采用各种相应的预防手段和措施,设置 IIS 把不必要的一些服务关掉以及设置 NTFS 的安全权限等:

1 设置 IIS

Internet Information Server 2000(IIS4.0)是运行在 Windows server 2000 上的信息服务软件,信息服务的安全性一直是人们关注的焦点,也是 IIS 重点解决的关键问题之一.它提供 FTP、WWW 等广泛使用的 Internet 服务.要做一个安全的站点,就要尽量少开或不开不必要的服务.现在一些站点的安全隐患就是由一些不必要的服务引起的.所以为了减少被黑客利用一些服务漏洞的机会,我们来把一些不必要的服务通通关闭.在“开始”菜单里的“程序”——>“管理工具”里选择“计算机管理”.在“服务和应用程序”里选择“服务” 我们把下面一些非常危险的服务全部关掉:

FTP publishing service

Telnet

Terminal Services

Remote Access Server

Remote Procedure Call (RPC) locater

关闭的方法是:在要关闭的服务上点右键——>“属性”, 点击常规菜单,再点击“停止”停止这个服务,然后把它的启动类型设置为“已禁用”.这样,

收稿日期:2005－01－10

作者简介:章海亮 (1977－),男,南昌人,华东交通大学讲师,主讲网络技术

一个服务就被你禁止了.当你把所有不必要的服务全部停止了以后,我们打开管理工具中的Internet服务管理器,删除"默认Web站点"及其下的所有目录,并且将这些文件全部从硬盘上彻底删除.删除C盘根目录下的Inetpub目录.

在"管理Web站点"上单击右键,选择"新建"——>"站点".根据提示输入你的站点名称,如输入web;点"下一步",输入您的网站的IP地址,如176.16.12.94;输入主目录的地址,如D盘根目录下的root目录;设定访问权限,只需要有"读取"权限就够了;然后单击"下一步"就完成了网站安装向导.

在刚建好的"web"站点"属性"里的"主目录"中设置"写入、脚本资源映射、目录浏览"权限为空.

2 帐号策略和密码策略

在windows 2000 server操作系统中,所有帐号的管理都在"计算机管理"——>"本地用户和组"里实现.

帐号策略:

1) 拥有Administrator权限的用户应该尽可能少.最好只有两个或者三个,设两个或者三个Administrator的原因是防止管理员一旦忘记其中一个帐号的口令还可以用另一个或两个备用帐号;另外如果被黑客攻破一个帐号并更改了口令还有机会在短时间内重新获得管理权.

2) 所有帐号应该严格管理,建立严格的分级审查制度,不要轻易给人特殊权限.

3) 将Administrator改名,改为一个不易猜测的名字.

将Guest帐号禁用,并且重命名为一个复杂的名字,并将其从Guest组删掉;有的黑客就是利用Guest的弱点,利用工具提升权限将一个帐户提升到管理员组的.

设置口令:

给所有用户设上复杂的口令,口令必须与帐号名不同,长度应该不低于8位,应该同时包含字母、数字和特殊字符.同时不要使用大家熟悉的单词(如admin)、熟悉的键盘顺序(如hjkl)、熟悉的数字(如2005)等.口令是黑客攻击的重点目标,口令一旦被突破管理员所做的任何安全设置都等于形如虚设,而这往往是不少网管所忽视的地方.

3 修改NTFS的安全权限

NTFS下所有文件默认情况下对所有人(everyone)为完全控制权限,这使黑客使用一般用户身份就能对文件做增加、删除、执行等操作.建议对一般用户只给予读取权限,而只给管理员和System完全控制的权限.

4 安全审核策略

在默认的情况下,windows2000是不记录登陆事件的.如果要想记录下黑客入侵事件就需要开启安全审核策略.如图1所示.

图1 审核策略

现在如果有人尝试对你的系统进行某些入侵(如口令猜测、改变帐户、访问未经许可的文件等)的时候,都会被记录在系统的安全日志里.

这样所有的事件都被记录在案,管理员只需要通过查看系统日志就会知道在哪个时间段内有哪些用户都干了些什么.如图2所示.

5 TCP/IP筛选

Windws2000 server TCP/IP筛选的功能.打开"网络和internet连接",在TCP/IP"属性"——>"高级"的"选项"里,选择"TCP/IP筛选".因为对外只需提

供 HTTP 服务,为了维护的需要还开了 FTP 服务,所以只需要允许 21、80 两个端口.

6　防火墙技术

防火墙技术是保证网络安全的重要屏障之一.它就象一个称职的门卫,守护在网络与 Internet 的交界处(即网关).它通过对任何企图进入网络的请求和信息进行论证和检查,并根据授权表来决定请求是否合法,进而决定下一步的操作.防火墙分为软件防火墙和硬件防火墙.目前较为流行的软件防火墙有天网防火墙,另还有一些著名的杀毒软件都具有防火墙的功能,如诺顿和瑞星杀毒软件等等.硬件防火墙功能强大,在大型网络中用的上,如校园网就必须有硬防火墙,以保证校园网的安全.

7　文件加密和硬盘数据还原

在对付黑客的所有方法之中,最保险的莫过于对重要信息和机密数据进行加密.加密能使文件中的信息全部变成密码.这样,即使黑客们突破了防火墙屏障,骗过了网络操作系统,他们也无法读懂和修改关键的数据.在安装系统时安装专业数据还原软件,如联想慧盾数据还原软件,万一数据被黑客更改或删除,也可重启计算机,使计算机数据能够得到还原.

8　总　结

网络安全问题是计算机网络的一个十分重要的问题,构建一个安全的网络服务器和采取可靠的安全措施是保证网络安全的重要内容.

参考文献:

[1] 黎连业.新编计算机计算机网络实用教程[M].北京:清华大学出版社.

[2] 欧　宇.如何创建 web 服务器[M].北京:中国农业大学出版社,2002.

[3] 彭　澎.计算机网络教程[M].北京:机械工业出版社,2002.

Investigate to Build a Security Web Serven

ZHANG Hai-liang

(East Chinatiao Tong University, Nanchang 330013, China)

Abstract: The security of computer network easily suffers from hacker's attacking. Wethod of using IIS4.0 to build web server is discussed in the paper. Some problems occurring in the process of setting webserver are well solved.

Key words: Computer network; security; IIS4.0