服务器安全性实验

【实验目的】

   通过实验掌握对Windows服务器系统IIS中Web服务器和FTP服务器进行安全配置的方法，以及他们的安全漏洞。

**【实验仪器】**

   安装Windows 2000系统的计算机，并且完全安装IIS服务。

【实验原理】

   IIS（Internet Information Server）是Windows系统中的Internet信息和应用程序服务器。利用IIS可以配置Windows平台方便地提供并且和Windows系统管理功能完美的融合在一起，使系统管理人员获得和Windows系统完全一致的管理。

  IIS常见漏洞包括idc&ida漏洞、htr漏洞、NT Site Server Adsamples漏洞、printer漏洞、Unicode解析错误漏洞、Webdav 漏洞等。因此，了解如何加强Web服务器，FTP服务器的安全性，防范由IIS漏洞造成的入侵就显得尤为重要。在下面的实验中通过对Web服务器和FTP服务器的安全配置，了解防范方法。

  我们可以手动进行IIS的安全配置，包括Web服务器，FTP服务器和SMTP服务器，也可以利用一些安全工具来进行。  
   IIS Lockdown是由微软开发的IIS安全配置工具，它按照模板的安全配置选项，通过关闭IIs服务器上的某些不必要的特性和服务，从而减少受攻击的威胁。此工具还与URLscan等协同工作，提供了多层次的防御和保护。

**【实验内容和步骤】**

实验步骤一：启动实验平台，拖出Windows2003Server PC机，并启动进入虚拟机环境，进入虚拟机环境，如图6-1所示：



                      图6-1 虚拟机界面

**步骤二:用IIS建立高安全性的Web服务器**

为保护Windows 2003系统的安全性，确认IIS与系统安装在不同的分区。如果IIS安装在系统分区，IIS的安全漏洞可直接威胁到系统的安全，建议卸载重新安装。

1）．删除不必要的虚拟目录

 打开“\*\wwwwroot”(其中 代表IIS安装的路径\*)，删除在IIS安装完成后，默认生成的目录，包括IISHelp，IISAdmin，IISSamples，MSADC等。这些默认生成的目录是众所周知的，容易给攻击者留下入侵的机会

2）．停止默认web站点

 打开“开始”->“管理工具”->“Internet信息服务(IIS)管理器”->“网站”，右键单击“默认网站”，在弹出的菜单中单击“停止”，根据需要启用自己创建的Web站点，如图6-2所示。默认web的根目录，默认在inetpub\wwwroot，还有其他一系列的参数设置也都是众所周知的，如果采用这些默认设置，将大大减小攻击难度。

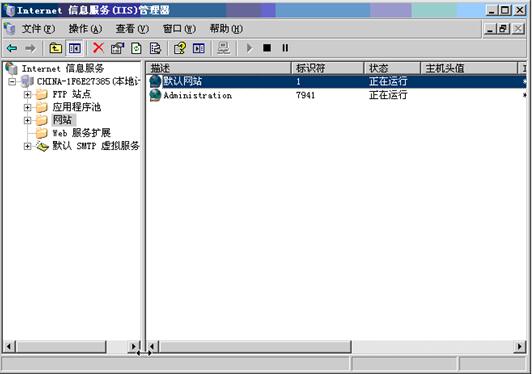


            图6-2  停止默认web站点，其用哪个自己的web站点

3）．IIS中的文件和目录进行分类，区别设置权限

   对于网站主目录中的文件和目录，单击目标右键，在“属性”中需要按需要给他们分配适当权限。一般情况下，静态文件允许读，拒绝写；ASP脚本文件，exe可执行程序等允许执行，拒绝读、写；通常不要开放写权限。此外，所有的文件和目录要将Everyone用户组的权限设置为只读权限。

4）．删除不必要的应用程序映射

在“Internet信息服务(IIS)管理器”中，右击默认网站，选择“属性”，如图6-3所示。

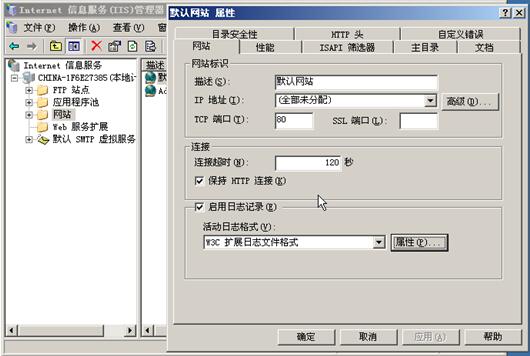


                     图6-3 属性示图

在网站目录属性对话框的“主目录”页面中，如图6-4所示，点击“配置“按钮。



                   图6-4 配置示图

在弹出“应用程序配置”对话框的“应用程序映射”页面，如图6-5所示，删除无用的程序映射。在大多数情况下，只需要留下 .asp一项即可，将.ida、.idq、.htr等全部删除，以避免利用这些程序映射存在的漏洞对系统进行攻击。



               图6-5  应用程序映射

5）.维护日志安全

在“Internet信息服务（IIS）管理器”中，-->“网站”，右击网站目录，选择“属性”。

    在网站目录属性对话框的“Web站点”页面中，在选中“启用日志记录”的情况下，点击旁边的“属性”按钮，如下图6-6所示：



                  图6-6 启用日志记录

在“常规属性”页面，点击“浏览”按钮或者直接在输入框中输入修改后的日志存放路径即可，如图6-7所示。

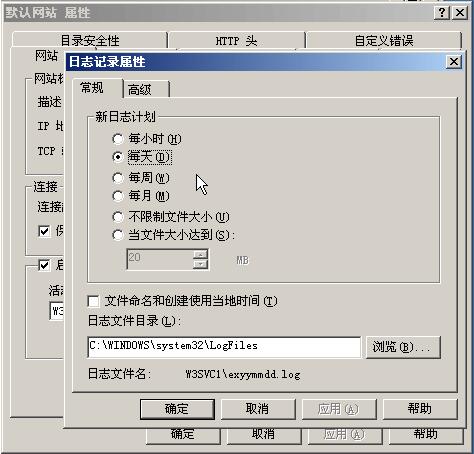


               图6-7  日志保存路径示图

修改路径后的日志文件要适当设置权限，它的文件权限建议administrator和system用户为完全控制，Everyone为只读；同时，建议与web主目录文件放在不同的分区，以增加攻击者利用路径浏览日志存放的路径难度，防止攻击者恶意篡改日志。

在网站目录属性对话框的“Web站点”页面中，如图6-16所示，Web服务器默认端口值为80，这是众所周知的，而端口号是攻击者可以利用的一个便利条件。将端口号改用其它值，可以增加安全性，当然也会给用户访问带来不便，系统管理员根据需要决定是否采用此条策略。

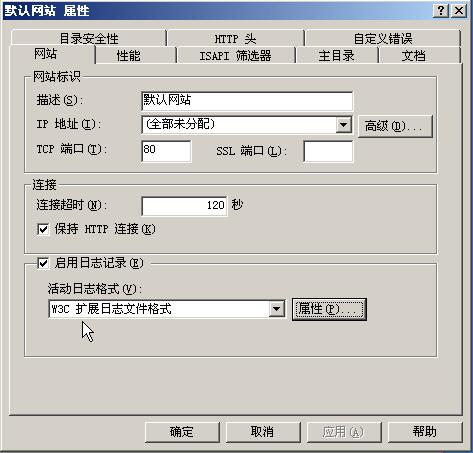


                 图6-8 修改端口值

    以上操作web服务器安全配置已基本完成。事实上，虽然这些安全配置可以在很大程度上提高我们的web服务器的安全性，但作为真正实用的web服务器，每天要接受大量的访问甚至大量的攻击，只有这些配置是远远不够的，还要采用一系列的安全措施，例如防火墙技术等，我们在后续实验中会陆续提到。

**步骤三： FTP服务器的安全配置**

1） 停止默认FTP站点

打开“控制面板”－>“管理工具”－>“Internet信息服务管(IIS)理器”，右击“默认FTP站点”，在弹出的菜单中点击“停止”，根据需要启用自己的FTP站点，如下图6-9所示。其目的也是要避免使用众所周知的默认服务器设置。



           图6-9停止默认ftp站点，其用哪个自己的ftp站点

FTP页面上，将TCP端口的“21”改为其它值

如下图6-10所示，FTP协议默认端口为21，改用其他的端口值使攻击者无法得到服务器的端口号从而增大了攻击难度，但同时也会给用户带来一定的不便。



                图6-10  修改端口值

启用日志记录

在FTP页面上，点中“启用日志记录”，如上图所示，单击“属性”，弹出下图6-11对话框。修改文件日志目录，将日志目录和FTP主目录分放在不同的路径下，并参照web服务器的权限设置，设置文件和文件目录的权限，以保护日志的安全性。



                 图6-11  日志目录

关于帐号

在帐号安全页面中，取消“允许匿名连接”选项，在“FTP站点操作员”只留下系统管理员一个帐号。如下图6-12所示。



                 图6-12账号安全示图

我们通过操作系统安全实验，已经配置了相对安全的管理员账号和密码。所以，我们在FTP站点操作员中只留下系统管理员，这就要求只有知道帐号和密码的用户才可以登录和管理FTP服务器，限制了匿名用户等其他用户的行为。

系统路径

在“主目录页面”设置FTP主目录，如下图6-13所示，注意该目录不要与系统路径在同一个磁盘分区，删除everyone用户组，设置其它用户的权限为可读，不可写，只对管理员用户保留完全控制权限。



               图6-13 设置FTP主目录

目录安全性

    在“目录安全性”页面中添加被拒绝或允许访问的IP。

在图6-14中，在选中“授权服务”的情况下，可以添加被拒绝的IP或IP组，其它未提到的IP视为允许访问。



                图6-14 目录安全性

    以上步骤对FTP服务器进行了一个初步的安全配置，更安全的FTP服务器配置由IISLockdown工具来完成

**【实验报告】**

1.记录系统各项安全设置前后的变化，并结合截图进行说明。

2.对Web服务器和FTP服务器做一个安全评测，并按照实验步骤对计算机进行安全配置，分析每一个步骤的设置原因。