IIS 安全加固

一【实验目的】

让学员通过该实验的练习主要掌握：

- 掌握 IIS 安全加固方式

二【实验环境】

- 操作机：Windows10

三【实验原理】

IIS 安全加固的六大技巧

技巧 1、安装系统补丁安装好操作系统之后，最好能在托管之前就完成补丁的安装,配置好网络后,如果是 2000 则确定安装上了 SP4,如果是 Windows Server 2003 系统，则最好安装上 SP1，然后点击开始→Windows Update，安装所有的关键更新。

技巧 2、设置端口保护和防火墙 Windows Server 2003 系统的端口屏蔽可以通过自身防火墙来解决，这样比较好，比筛选更有灵活性，桌面—>网上邻居—>(右键)属性—>本地连接—>(右键)属性—>高级—>(选中)Internet 连接防火墙—>设置，把服务器上面要用到的服务端口选中 即可。例如：一台 WEB 服务器，要提供 WEB(80)、FTP(21)服务及远程桌面管理(3389)在“FTP 服务器”、“WEB 服务器(HTTP)”、“远程桌面”前面打上对号如果你要提供服务的端口不在里面，你也可以点击“添加”铵钮来添加，具体参数可以参照系统里面原有的参数。然后点击确定。注意：如果是远程管理这台服务器，请先确定远程管理的端口是否选中或添加。

技巧 3、合理的权限设置 需要重点设置如下三种权限：WINDOWS 用户，在 WINNT 系统中大多数时候把权限按用户(組)来划分。在【开始→程序→管理工具→计算机管理→本地用户和组】管理系统用户和用户组。NTFS 权限设置，请记住分区的时候把所有的硬盘都分为 NTFS 分区，然后我们可以确定每个分区对每个用户开放的权限。【文件(夹)上右键→属性→安全】在这里管理 NTFS 文件(夹)权

限。IIS 匿名用户，每个 IIS 站点或者虚拟目录，都可以设置一个匿名访问用户(现在暂且把它叫“IIS 匿名用户”)，当用户访问你的网站的.ASP 文件的时候，这个.ASP 文件所具有的权限，就是这个“IIS 匿名用户”所具有的权限。设置好上述用户和文件系统权限后，还要记住设置如下的磁盘权限，设置原则如下：系统盘及所有磁盘只给 Administrators 组和 SYSTEM 的完全控制权限系统盘\Documents and Settings 目录只给 Administrators 组和 SYSTEM 的完全控制权限系统盘\Documents and Settings\All Users 目录只给 Administrators 组和 SYSTEM 的完全控制权限系统盘\Inetpub 目录及下面所有目录、文件只给 Administrators 组和 SYSTEM 的完全控制权限系统盘\Windows\System32\cacls.exe、cmd.exe、net.exe、net1.exe 文件只给 Administrators 组和 SYSTEM 的完全控制权限。

技巧 4、禁用不必要的服务操作路径为:开始菜单—>管理工具—>服务 Print Spooler Remote Registry TCP/IP NetBIOS Helper Server 以上是在 Windows Server 2003 系统上面默认启动的服务中禁用的，默认禁用的服务如没特别需要的话不要启动。

技巧 5、卸载不安全的组件最简单的办法是直接卸载后删除相应的程序文件。将下面的代码保存为一个.BAT 文件，(以下均以 WIN2000 为例，如果使用 Windows Server 2003 系统，则系统文件夹应该是 C:\WINDOWS\ )

```
regsvr32/u C:\WINNT\System32\wshom.ocx del C:\WINNT\System32\wshom.ocx
regsvr32/u C:\WINNT\system32\shell32.dll del C:\WINNT\system32\shell32.dll
```

然后运行一下，WScript.Shell, Shell.application, WScript.Network 就会被卸载了。可能会提示无法删除文件，不用管它，重启一下服务器即可。

技巧 6、IIS 服务器安全的防护原则一般情况下，黑客总是瞄准论坛等程序，因为这些程序都有上传功能，他们很容易的就可以上传 ASP 木马，即使设置了权限，木马也可以控制当前站点的所有文件了。另外，有了木马就然后用木马上传提升工具来获得更高的权限，我们关闭 shell 组件的目的很大程度上就是为了防止攻击者运行提升工具。如果论坛管理员关闭了上传功能，则黑客会想办法获得超管密码，比如，如果你用动网论坛并且数据库忘记了改名，人家就可以直接下载你的数据库了，然后距离找到论坛管理员密码就不远了。作为管理员，我们首

先要检查我们的 ASP 程序，做好必要的设置，防止网站被黑客进入。另外就是防止攻击者使用一个被黑的网站来控制整个服务器，因为如果你的服务器上还为朋友开了站点，你可能无法确定你的朋友会把他上传的论坛做好安全设置。这就用到了前面所说的那一大堆东西，做了那些权限设置和防提升之后，黑客就算是进入了一个站点，也无法破坏这个网站以外的东西。

四【实验步骤】

（1）首先打开计算机控制面板，选择“程序”，点击“启用或关闭 Windows 功能”。如下图 1 所示。

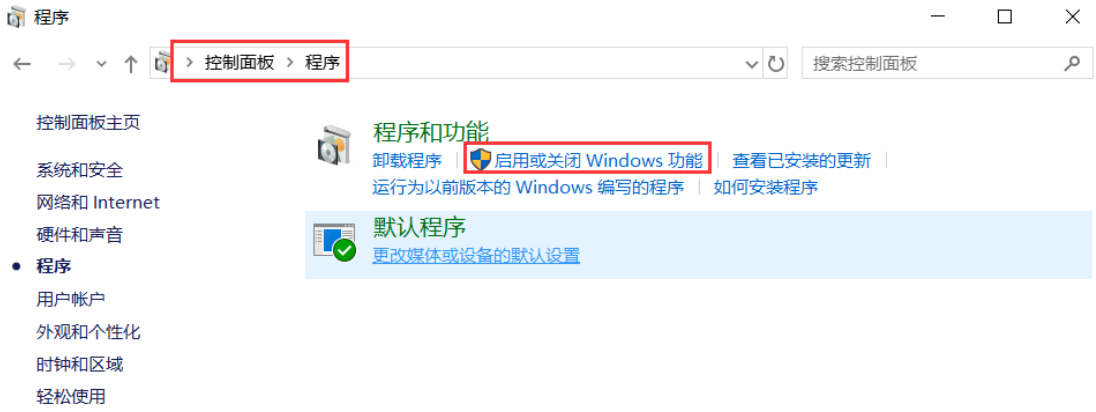

图 1

（2）在“Windows 功能”对话框中，点击“Internet Information Services”→“万维网服务”→“安全性”。勾选“IP 安全”，勾选“请求筛选”，点击“确定”按钮。如下图 2 所示。

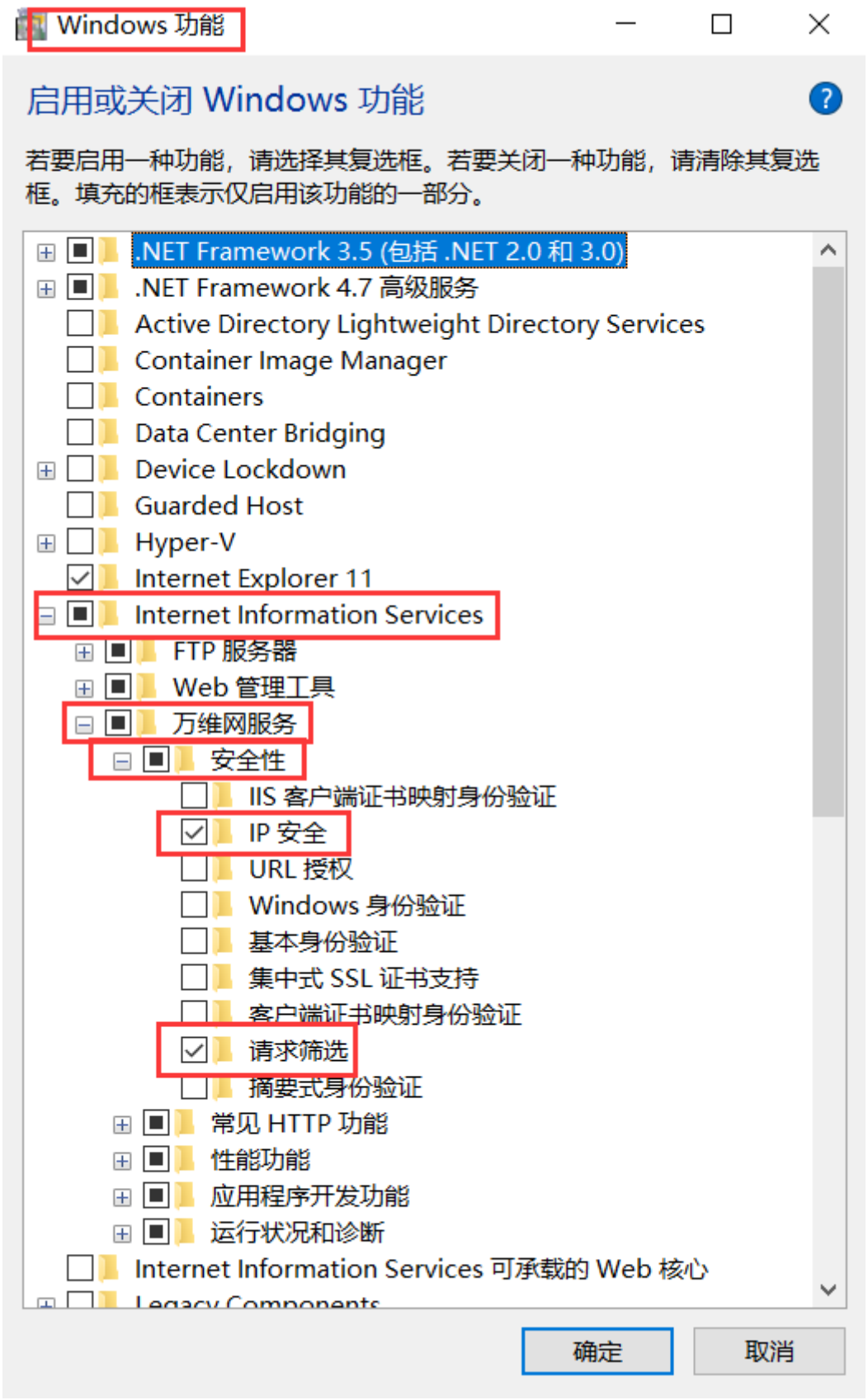

图 2

（3）首先需要查看 IIS 的版本信息，点击 IIS 管理器主页面上方【帮助】->【关

于 Internet 信息服务】。如下图 3 所示。

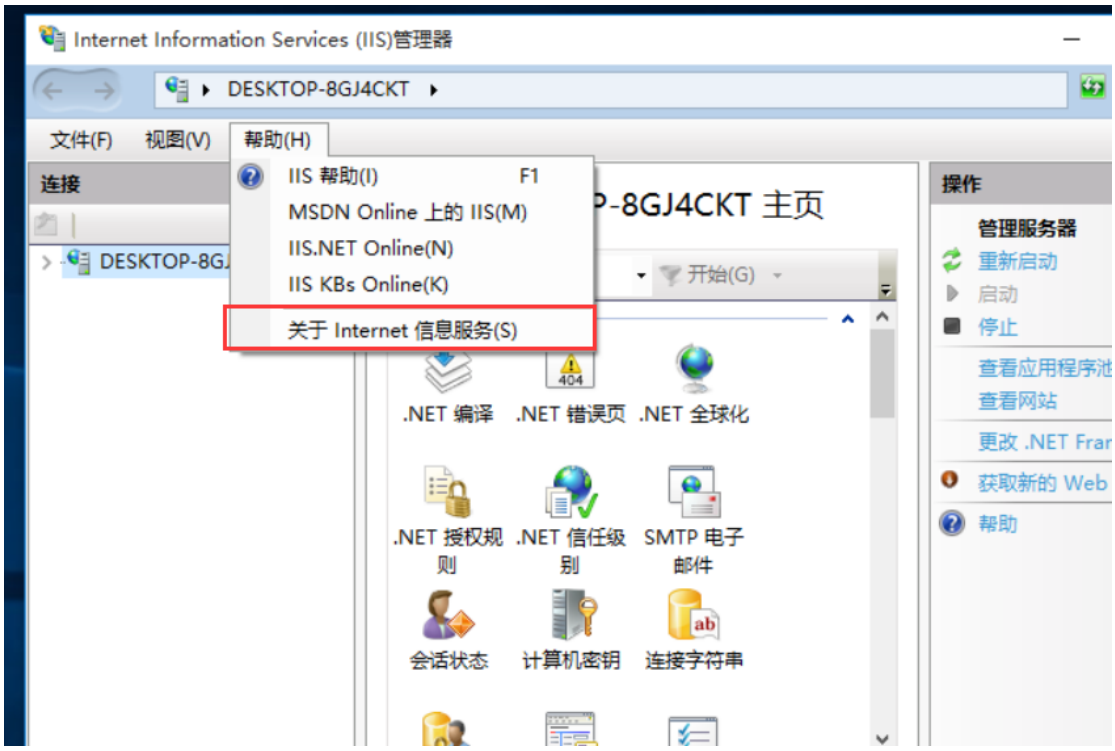

图 3

（4）可以看到主机的相关信息与 IIS 的版本信息。如下图 4 所示。

图 4

（5）IIS 安装后自带的默认网站具有很大的安全风险，建议删除或者禁用。右键网站，点击【删除】可以删除该网站。如下图 5 所示。

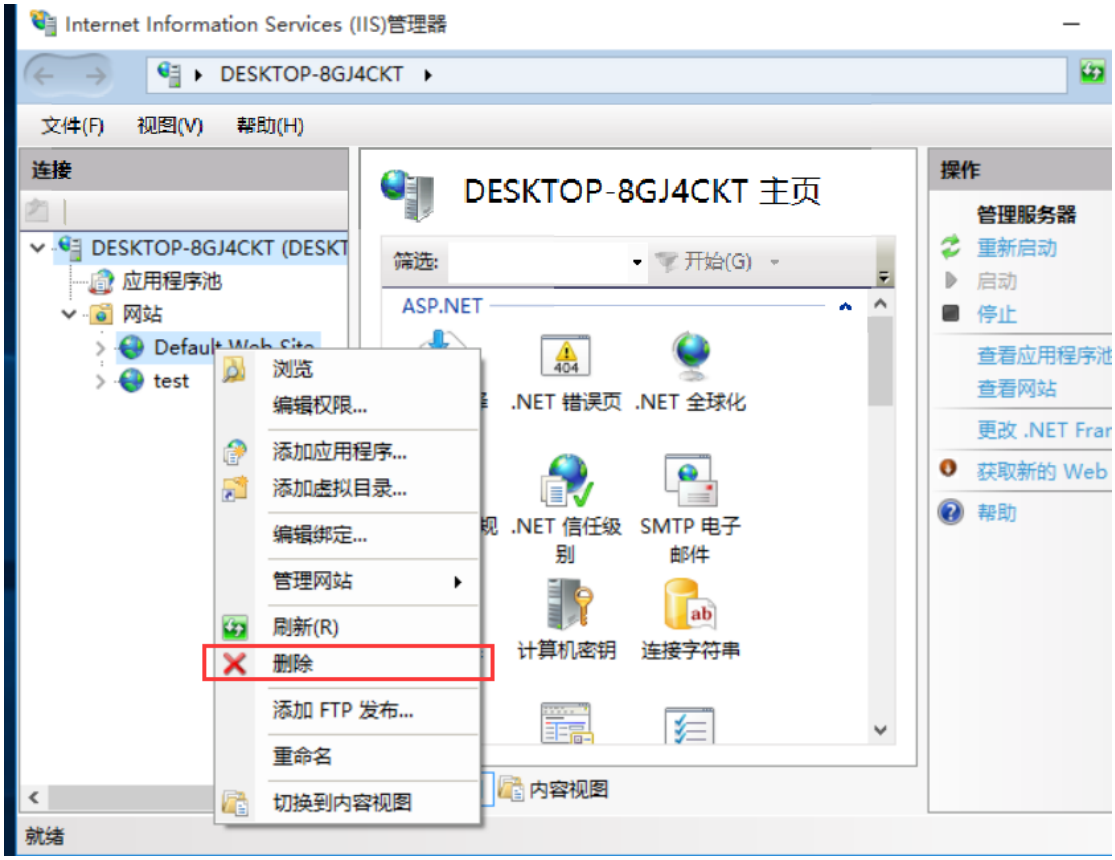

图 5

（6）网站返回的错误信息可以暴露服务器的相关信息，可能被攻击者利用。可以点击主页中的【错误页】更改错误信息。如下图 6 所示。

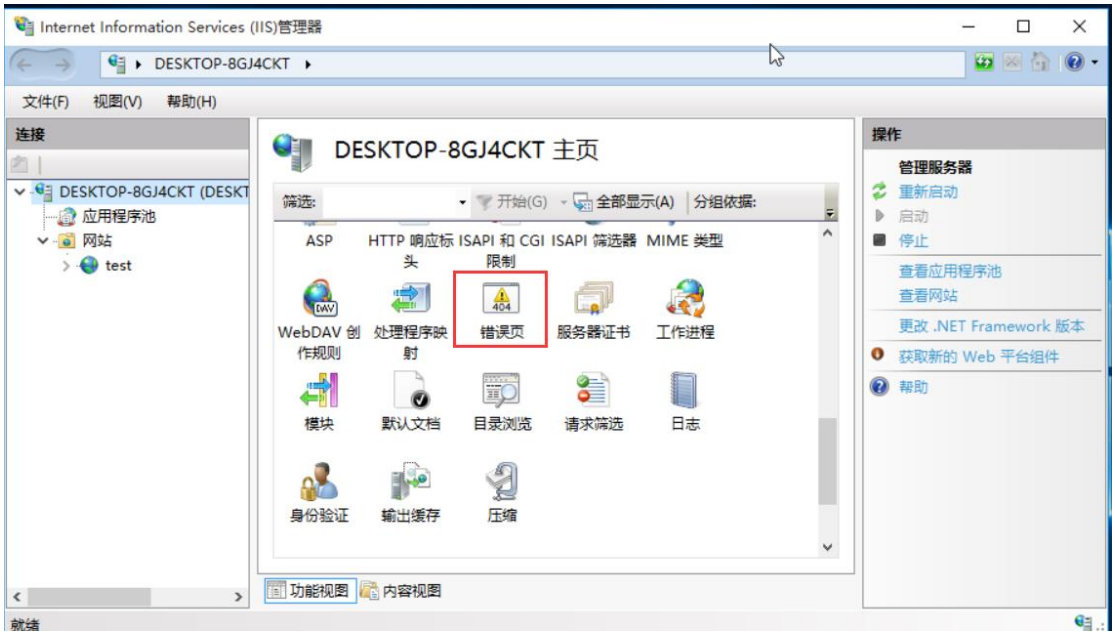

图 6

（7）可以看到每个错误信息对应的状态代码和路径，类型等信息。如下图 7 所

示。

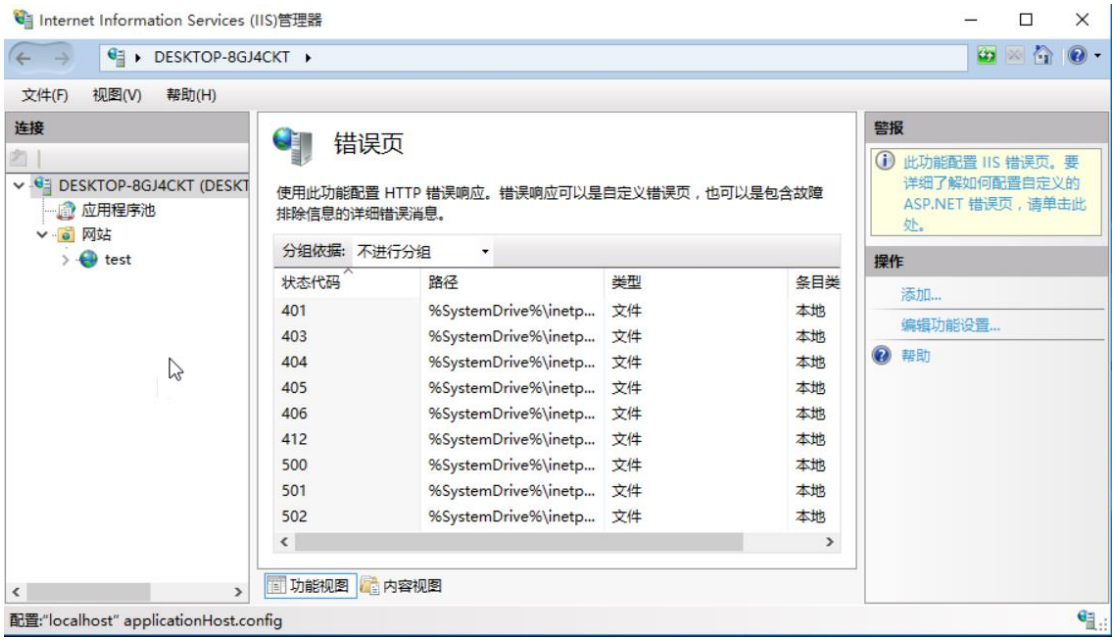

图 7

（8）点击某一状态代码可以编辑自定义错误页，可以在该页面更改状态代码，或自行设定响应操作。如下图 8 所示。

图 8

（9）IIS 管理器中也提供了 IP 地址和域限制功能，点击主页面中的相关选项可以进行设置。如下图 9 所示。

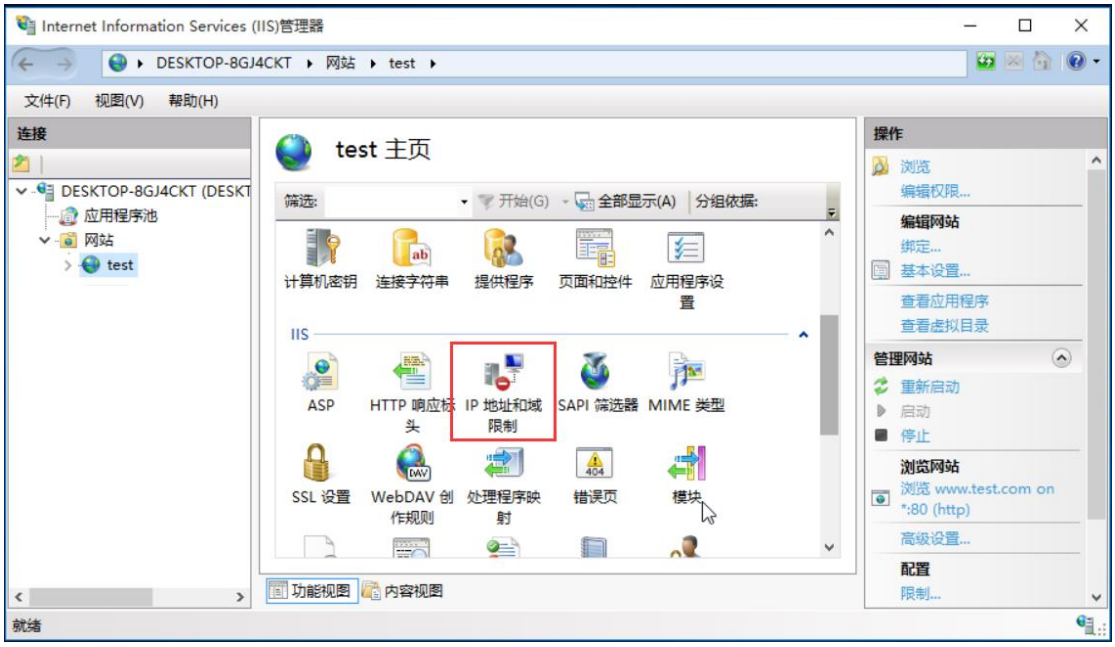

图 9

（10）点击【添加拒绝条目】可以对 IP 地址或域进行访问限制。如下图 10 所示。

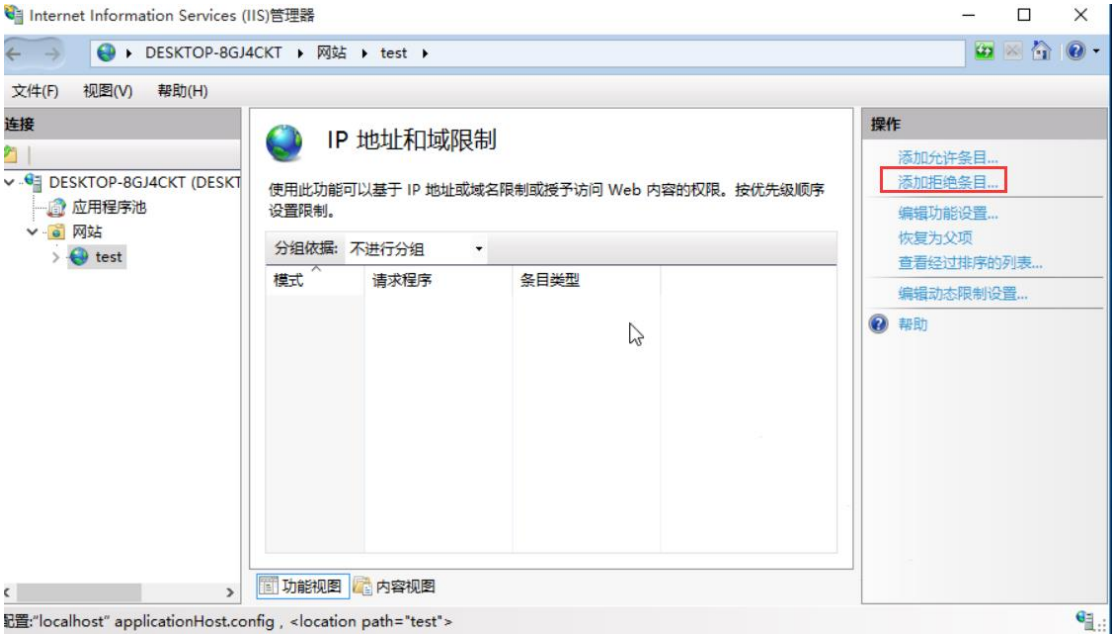

图 10

（11）可以限制某一特定 IP 地址的访问，也可以设定 IP 地址范围，点击【确定】使更改生效。如下图 11 所示。

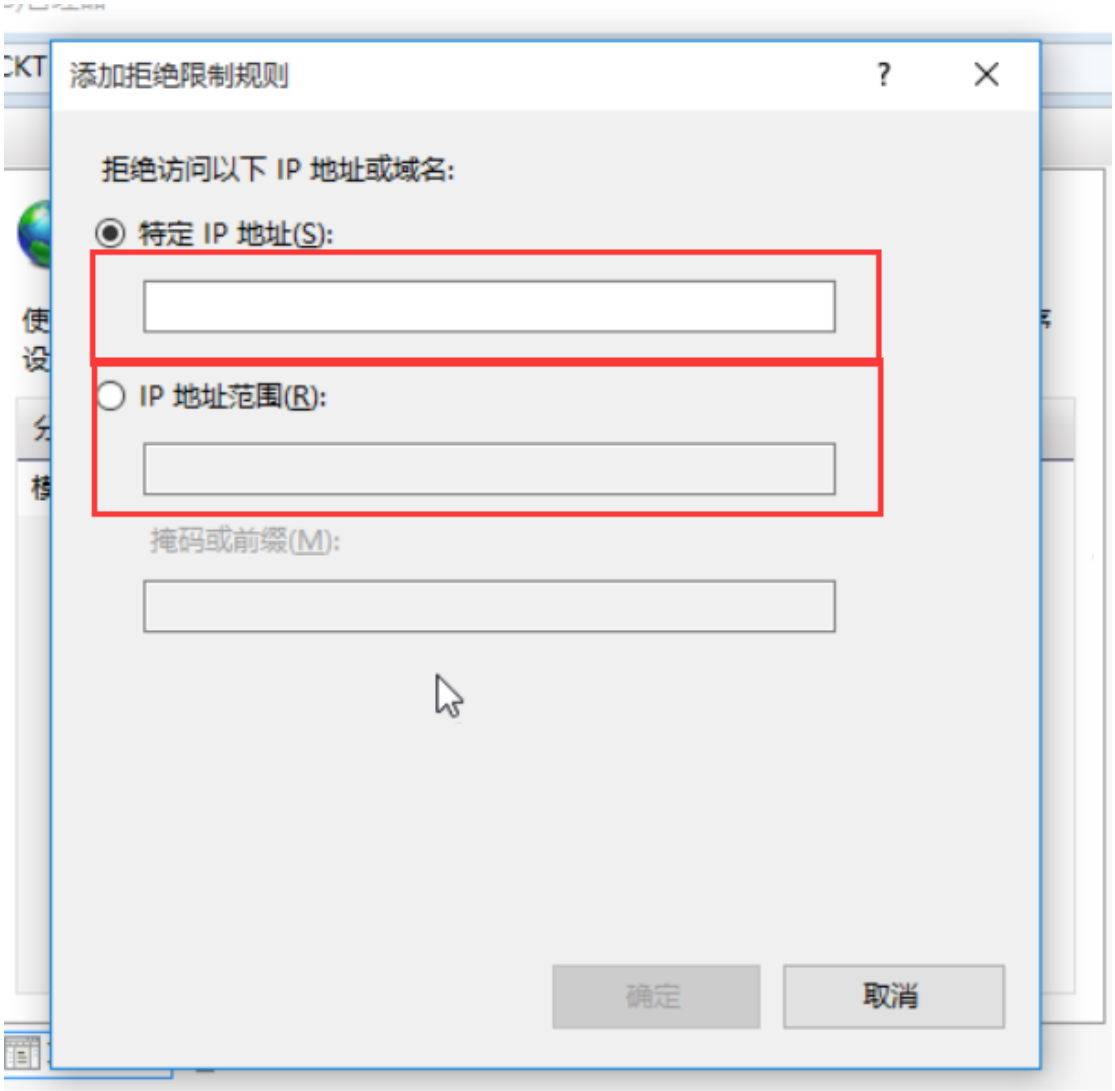

图 11

（12）用户访问服务器时返回的 HTTP 数据包头也包含很多信息，可能被攻击者利用，点击【HTTP 响应标头】可以设置标头信息。如下图 12 所示。

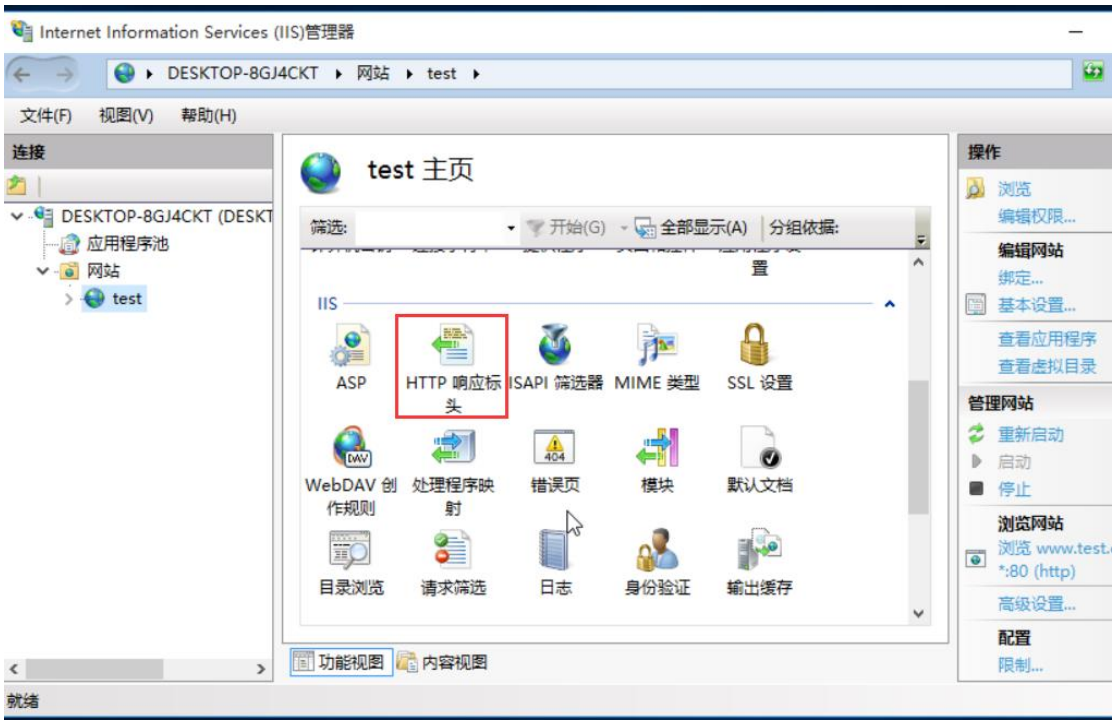

图 12

（13）点击标头可以编辑自定义 HTTP 响应头，可以更改名称和值。点击【确定】使更改生效。如下图 13 所示。

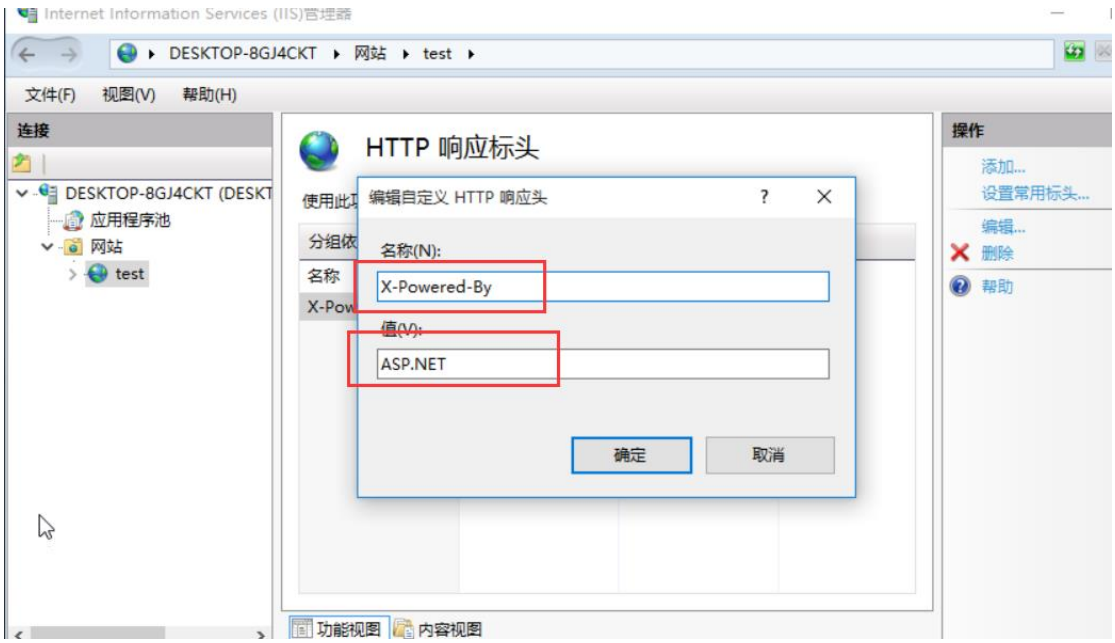

图 13

（14）服务器中也包含许多代码模块，一些可能包含漏洞被攻击者利用，点击【模块】管理 IIS 中的代码模块。如下图 14 所示。

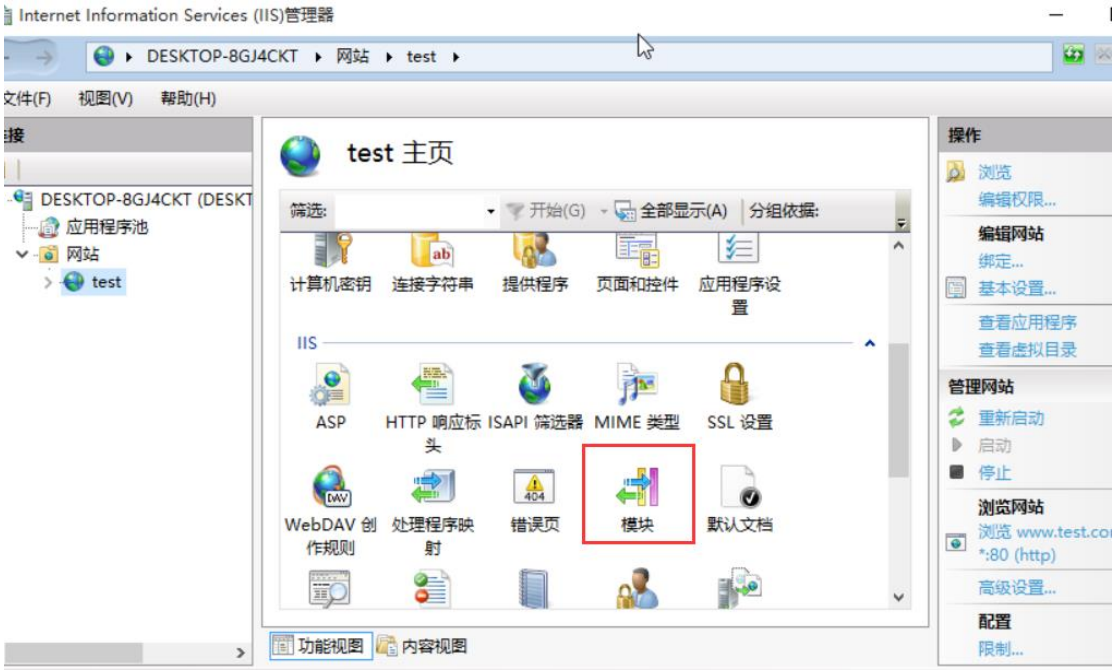

图 14

（15）点击某一模块，可以选择进行相关操作，比如添加托管模块，删除模块等。如下图 15 所示。

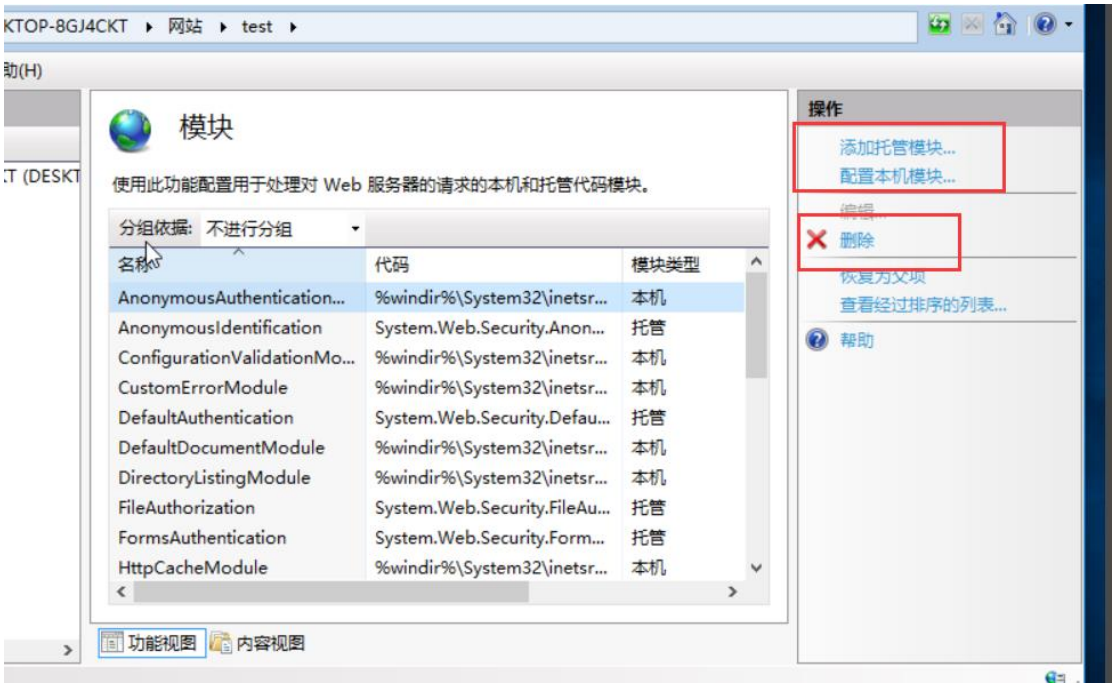

图 15

（16）点击【请求筛选】功能，可以添加对于文件的筛选过滤。如下图 16 所示。

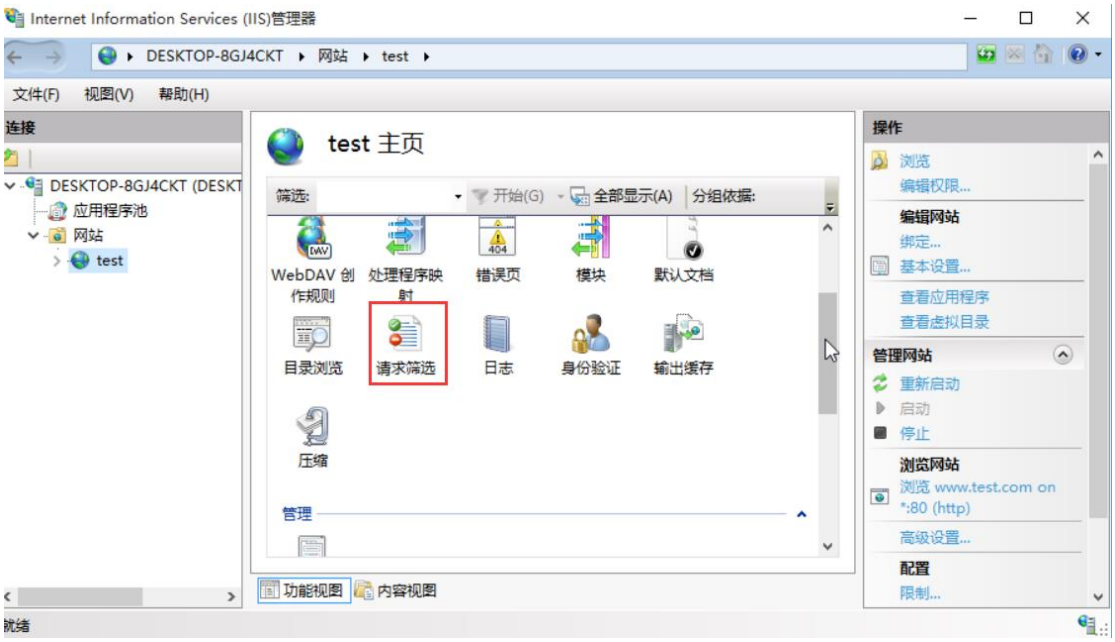

图 16

（17）点击某一文件扩展名，可以选择是否允许该类型文件的访问，或者删除该条规则。如下图 17 所示。

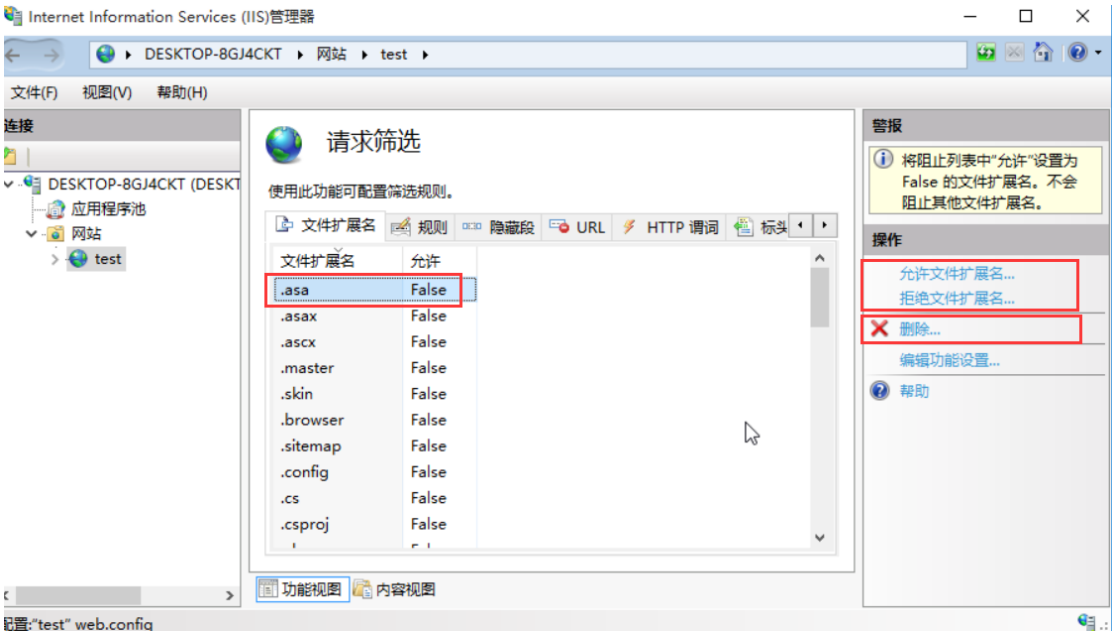

图 17

（18）IIS 管理器还提供了许多安全配置功能，学员可以自己摸索或查找相关资料，对 IIS 服务器进行进一步安全加固。

五【实验总结】

本实验介绍了 IIS 服务器安全加固的方式，希望学员掌握 IIS 服务器常见的加固方式，了解 IIS 安全防护的基本原理。