




i春秋:高风险之应用错误配置和默认配置

原创

喜欢散步  于 2015-06-01 08:50:26 发布  1238  收藏

文章标签: [入侵](#) [初学](#) [安全](#) [渗透](#) [漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/hope_smile/article/details/46299811

版权

实验环境

- 实验环境
 - 操作机: Windows XP
 - 目标机: Windows 2003
- 目标网址: 172.16.12.2
- 实验工具:
 - 中国菜刀
 - IISWrite
 - IISPUTScanner

实验目的

本节课程带领大家了解应用错误配置/默认配置所造成的危害, 通过实际演示, 学习应对此种危害的防御策略。

实验思路

- 1.扫描目标IIS写入权限
- 2.利用IIS写权限写入Webshell
- 3.理论方案
- 4.写权限漏洞修补

实验步骤

1

扫描目标IIS写入权限

打开浏览器,在地址栏中输入目标站点地址为 172.16.12.2回车显示是建设中的IIS服务器。

小提示:

- Internet Information Services (IIS, 互联网信息服务), 是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。IIS是一个World Wide Web server。Gopher server和FTP server全部包容在里面。 IIS意味着你能发布网页, 并且有ASP (Active Server Pages)、JAVA、VBscript产生页面, 有着一些扩展功能。IIS支持一些有趣的东西, 像有编辑环境的界面 (FRONTPAGE)、有全文检索功能的 (INDEX SERVER)、有多媒体功能的 (NET SHOW) 其次,IIS是随Windows NT Server 4.0一起提供的文件和应用程序服务器, 是在Windows NT Server上建立Internet服务器的基本组件。它与Windows NT Server完全集成, 允许使用Windows NT Server内置的安全性以及NTFS文件系统建立强大灵活的Internet/Intranet站点。

打开IISPutScanner.exe应用扫描服务器,输入startIP172.16.12.2和endIP172.16.12.2(也可以对一个网段进行设置),点击Scan进行扫描,PUT为YES服务器类型为IIS,说明可能存在IIS写权限漏洞。



利用IIS写权限写入Webshell

打开桌面下的iiswrite.exe应用,使用此软件来利用IIS写权限漏洞上传一句话木马。

写一个一句话asp的Webshell,request中的内容123为密码,保存文件为muma.txt。

小提示:

OPTIONS返回的是服务器的各种信息。

GET是返回的 cookie 信息。

HEAD是返回的头部信息。

DELETE是删除数据包。

PUT是上传数据包,是以文件的类型上传。

POST是以表单的形式上传。

COPY是复制数据包。

MOVE是改名数据包。

本次的实验是以PUT方式上传muma.txt文件。检查目标网站是否有test.txt文件显示出错,说明没有test.txt文件,那么我们可以请求的文件名可以为test.txt。域名为172.16.12.2,点击提交数据包。重新访问172.16.12.2/test.txt显示上传内容,说明上传成功。

使用COPY方式复制一份数据,数据的文件名为shell.asp,点击提交数据。使用浏览器访问http://172.16.12.2/shell.asp发现访问成功,没有出错,说明复制成功。

打开中国菜刀,鼠标右键点击添加输入地址http://172.16.12.2/shell.asp密码为123点击添加。双击打开连接,获取到服务器的目录,看到有上传的shell.asp文件和 test.txt文件。

理论方案

1.修改默认配置

2.修改默认密码

写权限漏洞修补

在C盘的根目录下有一个pass.txt文件,记录了服务器的用户名(administrator)和登陆密码(33gnd6nj),我们可以使用远程登陆验证是否正确,在运行输入mstsc回车。输入刚才找到的pass.txt文件里的用户名为(administrator)和登陆密码(33gnd6nj),点击确认。登陆成功,说明pass.txt文件密码和用户名正确.那就可以修改服务器的配置,来修改ISS漏洞。

点击开始,选择管理工具中Internet信息服务(IIS)管理器,首先点击Web服务器然后点击禁止,点击是关闭WebDAV,点击网络旁边的加号图标点击默认网站选中属性点击,点击主目录,取消勾选写入,点击应用,再点击确定。

点击默认网站选中权限,点击Internet来宾账号,然后取消勾选,只保留读取权限,然后点击确认。

使用IIS PUT Scanner v1.3重新扫描显示PUT上传显示为NO,说明不能上传。使用ISS write测试,使用PUT方式,提交数据包,显示501 错误信息,上传失败,说明修复漏洞成功。