[**IIS日志分析方法及工具**](http://www.cnblogs.com/xugang/archive/2007/09/21/901143.html)

       日志的重要性已经越来越受到程序员的重视,IIS的日志更是不言而喻。  
  
        IIS日志建议使用W3C扩充日志文件格式，这也是IIS 5.0已上默认的格式，可以指定每天记录客户IP地址、用户名、服务器端口、方法、URI资源、URI查询、协议状态、用户代理，每天要审查日志。如图1所示。    
   
  
  
IIS 的WWW日志文件默认位置为 %systemroot%\system32\logfiles\w3svc1\，（例如：我的则是在 C:\WINDOWS\system32\LogFiles\W3SVC1\），默认每天一个日志。  
  
建议不要使用默认的目录，更换一个记录日志的路径，同时设置日志访问权限，只允许管理员和SYSTEM为完全控制的权限。   如图2所示。  
  
  
  
  
如果发现IIS日志再也不记录了，解决办法：  
看看你有没有启用日志记录：你的网站--> 属性 -->“网站”-->“启用日志”是否勾选。  
  
日志文件的名称格式是：ex+年份的末两位数字+月份+日期。  
( 如2002年8月10日的WWW日志文件是ex020810.log ）  
  
IIS的日志文件都是文本文件，可以使用任何编辑器或相关软件打开，例如记事本程序，AWStats工具。  
  
开头四行都是日志的说明信息  
  
#Software        生成软件  
#Version         版本  
#Date            日志发生日期  
#Fields          字段，显示记录信息的格式，可由IIS自定义。  
  
日志的主体是一条一条的请求信息，请求信息的格式是由#Fields定义的，每个字段都有空格隔开。  
  
字段解释  
  
data                   日期  
time                    时间  
cs-method          请求方法  
cs-uri-stem         请求文件  
cs-uri-query       请求参数  
cs-username       客户端用户名  
c-ip                    客户端IP  
cs-version          客户端协议版本  
cs(User-Agent)  客户端浏览器  
cs(Referer)         引用页  
  
下面列举说明日志文件的部分内容（每个日志文件都有如下的头4行）：   
#Software: Microsoft Internet Information Services 6.0  
#Version: 1.0  
#Date: 2007-09-21 02:38:17  
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status  
  
2007-09-21 01:10:51 10.152.8.17 - 10.152.8.2 80    
GET /seek/images/ip.gif - 200 Mozilla/5.0+(X11;+U;+Linux+2.4.2-2+i686;+en-US;+0.7)   
  
　　上面各行分别清楚地记下了远程客户端的：  
  
            连接时间               2007-09-21 01:10:51  
                 IP地址              10.152.8.17 - 10.152.8.2     
                端    口               80  
            请求动作               GET /seek/images/ip.gif - 200  
            返回结果               - 200 （用数字表示，如页面不存在则以404返回）  
        浏览器类型              Mozilla/5.0+  
系统等相关信息              X11;+U;+Linux+2.4.2-2+i686;+en-US;+0.7  
  
  
附：IIS的FTP日志  
  
IIS的FTP日志文件默认位置为%systemroot%\system32\logfiles\MSFTPSVC1\，对于绝大多数系统而言（如果安装系统时定义了系统存放目录则根据实际情况修改）则是C:\winnt\system32\logfiles\ MSFTPSVC1\，和IIS的WWW日志一样，也是默认每天一个日志。日志文件的名称格式是：ex+年份的末两位数字+月份+日期，如2002年8月10日的WWW日志文件是ex020810.log。它也是文本文件，同样可以使用任何编辑器打开，例如记事本程序。和IIS的WWW日志相比，IIS的FTP日志文件要丰富得多。下面列举日志文件的部分内容。   
  
#Software: Microsoft Internet Information Services 6.0  
#Version: 1.0   
#Date: 2002-07-24 01:32:07   
#Fields: time cip csmethod csuristem scstatus   
03:15:20 210.12.195.3 [1]USER administator 331　   
（IP地址为210.12.195.2用户名为administator的用户试图登录）   
  
03:16:12 210.12.195.2 [1]PASS - 530　（登录失败）  
  
03:19:16 210.12.195.2 [1]USER administrator 331　   
（IP地址为210.12.195.2用户名为administrator的用户试图登录）   
  
03:19:24 210.12.195.2 [1]PASS - 230　（登录成功）   
03:19:49 210.12.195.2 [1]MKD brght 550　（新建目录失败）   
03:25:26 210.12.195.2 [1]QUIT - 550　（退出FTP程序）   
  
有经验的用户可以通过这段FTP日志文件的内容看出，来自IP地址210.12.195.2的远程客户从2002年7月24日3：15开始试图登录此服务器，先后换了2次用户名和口令才成功，最终以administrator的账户成功登录。这时候就应该提高警惕，因为administrator账户极有可能泄密了，为了安全考虑，应该给此账户更换密码或者重新命名此账户。  
  
如何辨别服务器是否有人曾经利用过UNICODE漏洞入侵过呢？可以在日志里看到类似如下的记录：    
如果有人曾经执行过copy、del、echo、.bat等具有入侵行为的命令时，会有以下类似的记录：   
13:46:07 127.0.0.1 GET /scripts/..＼../winnt/system32/cmd".exe 401   
13:46:07 127.0.0.1 GET /scripts/..＼../winnt/system32/cmd".exe 200    
13:47:37 127.0.0.1 GET /scripts/..＼../winnt/system32/cmd".exe 401   
  
  
相关软件介绍：  
  
        如果入侵者技术比较高明，会删除IIS日志文件以抹去痕迹，这时可以到事件查看器看来自W3SVC的警告信息，往往能找到一些线索。当然，对于访问量特别大的Web服务器，仅靠人工分析几乎是不可能的--数据太多了！可以借助第三方日志分析工具，如Faststs Analyzer、Logs2Intrusions v.1.0等。此处仅仅介绍一下Logs2Intrusions日志分析工具。它是一个由Turkish Security Network公司开发的自由软件，是免费的日志分析工具，可以分析IIS 4/5、Apache和其他日志文件。可以到<http://www.trsecurity.net/logs2intrusions>下载最新的版本。该软件简单易用，下面是它的主界面，如图3所示。   
  
  
  
  
单击【Select】按钮后选择要分析的日志文件，然后单击【Next】按钮，在出现的窗口中单击【Begin Work】按钮即可开始分析，如图4所示。    
  
  
  
  
如图4所示，它表明已经发觉入侵的痕迹。如果没有发现痕迹则弹出如图5所示的对话框。    
  
  
  
  
在发现痕迹后单击【Next】按钮继续，如图6所示。   
  
  
  
  
【View Report】按钮是查看报告，【Save Report】按钮是保存报告，【New Report】按钮是生成新报告。下面是报告的例子，如图7所示。   
  
  
  
  
在"Intrusion Attempt"列中列出了超链接，选择它可以得到Trsecurity公司的专家的建议。和该软件同一目录中的sign.txt是入侵行为特征的关键字，用户可以根据新的漏洞的发现而随时补充。