Webshell

1.webshell简介

webshell，顾名思义：web指的是在web服务器上，而shell是用脚本语言编写的脚本程序，webshell就是就是web的一个管理工具，可以对web服务器进行操作的权限，也叫webadmin。webshell一般是被网站管理员用于网站管理、服务器管理等等一些用途，但是由于webshell的功能比较强大，可以上传下载文件，查看数据库，甚至可以调用一些服务器上系统的相关命令（比如创建用户，修改删除文件之类的），通常被黑客利用，黑客通过一些上传方式，将自己编写的webshell上传到web服务器的页面的目录下，然后通过页面访问的形式进行入侵，或者通过插入一句话连接本地的一些相关工具直接对服务器进行入侵操作。

2.如何上传webshell

<1>.解析漏洞上传

现在对于不同的web服务器系统对应的有不同的web服务端程序，windows端主流的有iis，linux端主流的有nginx。这些服务对搭建web服务器提供了很大的帮助，同样也对服务器带来隐患，这些服务器上都存在一些漏洞，很容易被黑客利用。

(1)iis目录解析漏洞

比如：/xx.asp/xx.jpg

虽然上传的是JPG文件，但是如果该文件在xx.asp文件夹下，那个iis会把这个图片文件当成xx.asp解析，这个漏洞存在于iis5.x/6.0版本。

(2)文件解析漏洞

比如：xx.asp;.jpg。在网页上传的时候识别的是jpg文件，但是上传之后iis不会解析;之后的字符，同样会把该文件解析成asp文件，这个漏洞存在于iis5.x/6.0版本。

(3)文件名解析

比如：xx.cer/xx.cdx/xx.asa。在iis6.0下，cer文件，cdx文件，asa文件都会被当成可执行文件，里面的asp代码也同样会执行。（其中asa文件是asp特有的配置文件，cer为证书文件）。

(4)fast-CGI解析漏洞

在web服务器开启fast-CGI的时候，上传图片xx.jpg。内容为：

  <?php fputs(fopen('shell.php','w'),'<?php eval($\_POST[shell])?>');?>

这里使用的fput创建一个shell.php文件，并写入一句话。访问路径xx.jpg/.php，就会在该路径下生成一个一句话木马shell.php。这个漏洞在IIS 7.0/7.5，Nginx 8.03以下版本存在。语言环境：PHP，prel，Bourne Shell，C等语言。

\*注：fast-CGI是CGI的升级版，CGI指的是在服务器上提供人机交互的接口，fast-CGI是一种常驻型的CGI。因为CGI每次执行时候，都需要用fork启用一个进程，但是fast-CGI属于激活后就一直执行，不需要每次请求都fork一个进程。比普通的CGI占的内存少。

(5)apache解析漏洞

apache解析的方式是从右向左解析，如果不能解析成功，就会想左移动一个，但是后台上传通常是看上传文件的最右的一个后缀，所以根据这个，可以将马命名为xx.php.rar，因为apache解析不了rar，所以将其解析为php，但是后台上传点就将其解析为rar，这样就绕过了上传文件后缀限制

<2>.截断上传

在上传图片的时候，比如命名1.asp .jpg(asp后面有个空格)，在上传的时候，用NC或者[burpsuite](http://www.91ri.org/4522.html" \o "利用burpsuite获得免费空间" \t "http://www.cnblogs.com/mujj/articles/_blank)抓到表单，将上传名asp后面加上%00（在burpsuite里面可以直接编辑HEX值，空格的HEX值为20，将20改为00），如果HEX为00的时候表示截断，20表示空格，如果表示截断的时候就为无视脚本中的JPG验证语句，直接上传ASP。

<3>.后台数据库备份

在一些企业的后台管理系统中，里面有一项功能是备份数据库（比如南方cms里面就有备份数据库的功能）。可以上传一张图片，图片里面含有一句话木马，或者将大马改成jpg格式，然后用数据库备份功能，将这张图片备份为asp等其他内容可以被解析为脚本语句的格式，然后再通过web访问就可以执行木马了，但是这种方法很老了，现在大多数的cms已经把这种备份的功能取消了，或者禁用了。

<4>.利用数据库语句上传

(1) mysql数据库into outfile

这种方式的前提必须是该网站有相应的注入点，而且当前用户必须要有上传的权限，而且必须有当前网页在服务器下的绝对路径。方法是用联合查询，将一句话木马导入到网站下边的一个php文件中去，然后使用服务端连接该网站。但是上述方法条件过于苛刻，一般遇到的情况很少。

(2)建立新表写入木马

一些开源cms或者自制的webshell会有数据库管理功能，在数据库管理功能里面有sql查询功能，先使用create table shell(codetext);创建一个名字叫做shell的表，表里面有列明叫做code，类型为text。然后使用insert into shell(code) values(‘一句话马’)，这里讲shell表中的code列赋值为一句话的马，然后通过自定义备份，将该表备份为x.php;x然后就被解析成为php然后执行了，这里不是x.php;x就一定能够解析为php，不同的web服务器上面的服务程序不同，然后过滤规则也不同，可能会使用其他的方式。

(3)phpMyadmin设置错误

phpMyadmin用来管理网站数据库的一个工具，其中config.inc.php为其配置文件，在查看的该文件的时候，如果$cfg[‘Servers’][$i][‘auth\_type’]参数的值设置没有设置（默认为config）说明在登陆数据库的时候没有做相应的验证，可以直接连入数据库，而且在Mysql在一些版本下面默认登陆都是以root用户进行登陆（即管理员），所以登陆进去为最大权限。但是root一般只能本地登陆，所以必须创建一个远程登陆用户。用远程登陆用户登陆之后，创建一个表，然后再将一句话木马写入。

3.关于webshell的隐藏

在上传webshell的时候必须要进行webshell的隐藏工作。隐藏webshell，第一个目的是不让网站管理员发现马将其删掉，第二个目的是为了不被其他的Hacker发现了这个文件并加以利用。

【不死僵尸】

windows系统存在系统保留文件名，windows不允许用这些名字来命名文件,因为这些名字都属于设备名称，等价于一个 DOS 设备，如果我们把文件命名为这些名字，Windows 就会误以为发生重名，所以会提示“不能创建同名的文件”等等。aux|prn|con|nul|com1|com2|com3|com4|com5|com6|com7|com8|com9|lpt1|lpt2|lpt3|lpt4|lpt5|lpt6|lpt7|lpt8|lpt。但是这些可以使用windows的copy命令创建与del删除,我们只要按照完整的 UNC 路径格式，就是网上邻居的路径格式，正确输入文件路径及文件名即可。

copy 3.asp [\\.\E:\aux.asp](\\\\.\\C:\\aux.asp)

Del \\.\E:\aux.asp

【注册表隐藏】

注册表路径：

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer＼Advanced\Folder\Hidden\SHOWALL

在这个路径下有一个CheckedValue的键值，把他修改为0，如果没有CheckValue这个key直接创建一个，将他赋值为0，然后创建的隐藏文件就彻底隐藏了，即时在文件夹选项下把“显示所有文件”也不能显示了。