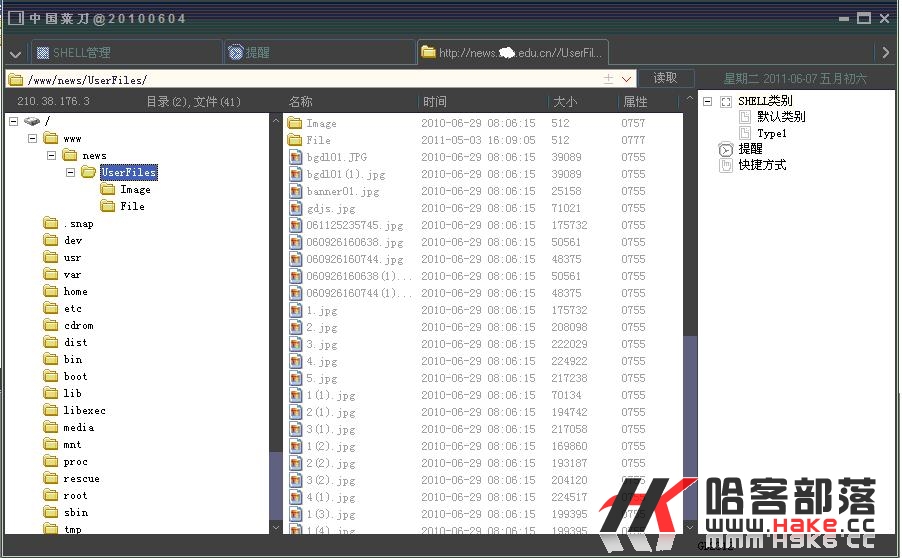
这个是目标站   看了下是用php做的  
  
用工具检查过没有注入这些高危漏洞， 主页不能直接拿下，就旁注，在主页的链接找到个站点，手工测试了下是同一服务器的，  
用软件检查过还是不存在注入，于是用工具扫描一下是否有漏洞页面可以利用  
  发现了外的收获扫描到一个漏洞链接  
  
  
[http://news.xxxx.edu.cn:80/editor/FCKeditor/editor/filemanager/upload/test.html](http://news.xxxx.edu.cn/editor/FCKeditor/editor/filemanager/upload/test.html) HTTP/1.1 200 OK  
  
直接找个php的小马上传   
  
提示成功 upload/asp.php    
马上打开小马  发现小马并没有上传成功， 于是找了张图片上传，提示成功 upload/1.jpg  
打开图片还是没有成功，估计是没有上传上去， 不知道是不是漏洞没哟，还是其他的原因  
看了扫描结果觉得既然存在这个漏洞链接为什么不存在其他的呢，这个编辑器漏洞也不少的，于是在用扫描器在扫描  
结果发现找到的漏洞页面多2个了，不知道什么原因，难道工具都会出错？反正结果是好事,  
  
[http://news.xxx.edu.cn:80/editor/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx](http://news.xxx.edu.cn/editor/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/aspx/connector.aspx)  
   
这个编辑器的利用，我不在行，我尝试新建目录，但是没有成功，这里有个上传了直接上传图片或者马，只提示正在上传，不知道是不是漏洞补了，Type=all&Connector=connectors/aspx/connector.aspx   这里改了不少还是没有成功上传马  
  
于是查看了一下版本是2.3的  在网上找相关的漏洞，发现了不少，直接用其中一个  
  
  
    1、漏洞利用  
上传脚本：  
<form id="frmUpload" enctype="multipart/form-data" action="http://news.xxx.edu.cn:80/editor/FCKeditor[/editor/filemanager/upload/php/upload.php?Type=Media](http://www.xxx.com/FCKeditor/editor/filemanager/upload/php/upload.php?Type=Media)" method="postt">  
Upload a new file:<br>  
<input type="f" name="N Fi " size="50"><br>  
<input id="btnUpload" type="submit" value="Upload">  
</form>   
    提交后查看源码就能看到上传文件的位置是upload/a.php    
由于不知道这个相对路径的从哪里开始的于是就从  [/editor/filemanager/upload/php/](http://www.xxx.com/FCKeditor/editor/filemanager/upload/php/upload.php?Type=Media) 这段目录一直猜，知道猜到网站根目录才猜对   由于这次是用菜刀 一句话的 打开了个空白页面 证明页面存在  然后用菜刀年纪  
   
看了下目录才发现是linux的服务器，由于ping不通，所以开始的时候就没有判断服务器是什么系统。拿下了才发现是linux的 目录翻了下，都能浏览，权限不小，但是没什么地方能修改的权限，找了不少连上传张正常的图片都不行，最好发现有两个upload的目录可以上传，于是估计是服务器设定了，于是上传了个php的目录 居然不能正常工作，   
  
不知道是不是linux的 这木马就不能工作了。原因没有找到，知道的同志希望教我一下。 linux 接触的很少，提权也不怎么会 ，还要到百度找linux提权的教程学习，之前都是win的提权，linux的不容易找到啊，服务器用扫描器扫描了下开放了22端口，能用linux的远程桌面，这部开放服务就能省下了，这个网站就暂时到这里  
  
本来想申请一下核心的，看有没有机会能进入，但是由于要学习，汇编和脚本还没入门呢，上网的时间都不够，不知道管理员可不可以放松一下条件