**文/图 残剑**

上次出了一篇。太阳张柏芝的文章,唉 后来有人依葫芦画瓢。柏芝姐姐就被各种xxoo。悲剧,听取某位建议。隐藏url, 话说黑阔们是见不得url的。不然又会手贱了- -…

这次的目标是某某理工大学。

目标:[www.xxx.net](http://www.xxx.net/)

首先对目标进行一个大致的踩点。

从主页的外观上看像某个cms。但是不确定程序。接着手工查找着网站的敏感信息。

在robots.txt上看到此网站是用phpcms3.0版本搭建的。



百度phpcms3.0已经公开的0day

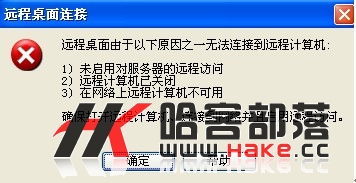


用虚拟机本地搭建了一个php环境。用公开的exp测试。上传提示: 上传格式错误.说明漏洞已经被管理员修补了这个漏洞。后又百度了几个exp,均宣告失败。主站渗透未果,接着进行旁注测试。用旁注查询工具查询,看到几个网站都是用phpcms3.0搭建的。Exp我就没去测试了,同个服务器同个程序,应该漏洞都是同样被修补了把。

纠结了许久,只好试试c段了。

(服务器因后来操作失误,被关机了。所以无截图。抱歉,)

利用注入进入了c段一网站后台。后台很简陋,始终拿不下shell。也可能是自身技术的问题把. 没找到一处可以利用的地方。拉进Wwwscan扫敏感目录。发现该网站有个bbs目录。就猜测bbs目录下是个论坛。访问之,拉到网站底部看版权信息知道网站是用动网的程序搭建的。点进板块一看,看到有个admin的用户发表的帖子。我想admin应该就是网站的管理员了。于是尝试弱口令进行登录。（不解释的说,rp太好了）.. ,成功登录。动网后台拿webshell:前台上传一个图片小马,后台数据库备份为.asp后缀的文件..一切轻车熟路。上传了个大马之后就开始提权。Ws组建在,我一看到这就心想有戏了。但ws在没用,还要用可读可写可执行exe文件的目录。在C:\recycler处,上传cmd。环境探测,发现主机支持aspx。直接传了个aspx大马上去,能执行基本的dos命令。丢了个pr执行命令,提权成功。随后连接3389.却怎么也连接不上



我以为是服务器更改了远程终端的端口。用注册表查了一下终端的键值。显示的是3389。端口没改,不过工具也有出错的时候,就打算自己手工来看看。Netstat –an 没发现有3389。就用2003开3389命令一行一行用cmd执行。再次netstat –an。这时候已经是开着了.连接！可还是一样的提示。想了想决定先重启下服务器试试。用shutdown -s -t 00 执行。服务器重启,大马自然也就连接不上了。过了许久不见服务器重启好,以为哪里出了问题。后来看了一下命令..刚刚执行的shutdown -s -t 00 是关机的意思。shutdown -r -t 00才是重启.擦,悲剧了。

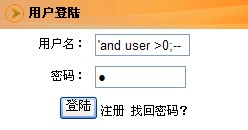
这台c段服务器算是报销了。哎,,搞了那么久毁在了一条命令上..真够蛋疼的。

没办法,,继续看别的c段服务器。

看到一个aspx的企业站,觉得会比较好拿就下手之~

简单踩点了一下,没发现任何aspx?id=形式的动态连接。

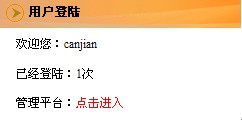
继续,,发现用个用户登录。测试下有没注入漏洞





出错。但随后测试,发现并不能注入。

那就按正常步骤来把。注册,登录之~



进入管理平台。

发表新留言发现有fck编辑器。



二次上传漏洞拿下webshell。

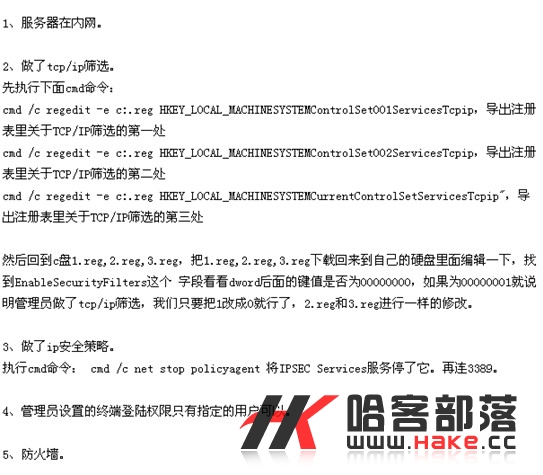
上大马。Ws存在,服务器支持aspx。用pr执行命令提权。浏览器进度条一直处于卡着的状态。哎,pr提权超时了。仍了个免参数的pr上去。成功！



看帐号就知道服务器已经被人日过了。纠结…

3389也开了。可还是和上一台服务器同样的情况。无法连接远程终端..百度搜索了一下3389开了不能连接的原因。

原帖: <http://tieba.baidu.com/f?kz=585376793>





最后测试了一下。还是连接不上。这时候就怀疑服务器用硬防了..阻止了外部ip连接3389..

后来搞得太迟,就去睡了 早上起来一直再想,为什么3389连不上, 试了挺多方法的。像啥,注册表导出查看tcp/ip筛选。端口转发, 终端还是无法连接

没办法 直接仍了一个远控上去拿到了两台服务器的权限。

(注：第二台服务器不是不让pr嘛？我用的是免参数的pr成功添加的帐号。但我是怎么上的远控呢?这里告诉大家一个小技巧。用c32打开免参数pr在十六进制下编辑。搜索net user。找到这一段。如图,





直接修改为远控的地址即可。

) 但是在远控上搞了一番,还是没能弄懂是什么情况- -|| 话说,我日c段是想上服务器cain的。但是没有登录终端..这就没办法实现了。本来想用zxarps在cmd下进行嗅探。但是1核的垃圾服务器 怕他卡死

所以没搞 有木有神人知道怎么搞可以pm我。 E-mail: [0day@hake.cc](mailto:0day@hake.cc)

重要的是渗透过程中的思路,全当自己做个记录把。