图/文

作者：人生

昨天，有点小事上面吩咐的事刚做完，只能继续搞完了。。。后来发下需要一套程序。就匆匆跑去弄了。

好了不废话

目标：[www.fuck.com](http://www.fuck.com/)

目标独立…

   系统LINUX 阿帕奇服务，但目标是另一个分站。查的内容也就是如下

直接用哈客的御剑旁下



直接C段查了一下。一个段。没一台机。这恶心。目标也太夸张了。而且也看不到分站。但明明有分站

然后只能跑主站看看，扫扫目录。虽然这很盲目，但也可以找到敏感信息。可以说什么都没扫到。就扫到了一些无用目录。。

然后我随便点，发现一个地方



发现下载地址是直接IP。然后带8080端口，然后直接删掉多余的内容



发现是个能访问的WEB. 居然发现是WIN的= =。话说这个WIN让我很高兴啊。。。。。

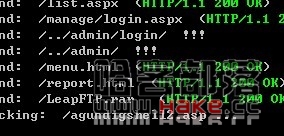
然后扫一下目录。

Win+.net

扫了很久。木啥利用。

找了个点。只判断数字。也没法注入，就放弃注入的念头了

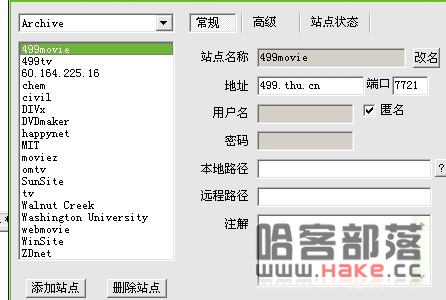
吃饭的时候放这扫。反正回来也有可能有惊喜。。



刚回来一下坐。NND，真的给我来个惊喜，发现个压缩包。然后下载下来。，

打开看看

是leapftp



发现都是些没用的。

选择第二个的时候发现了几个是他的服务器的IP



但，怎么连也连不上。也只能放弃了。。。。思路开始断了。也很无语。

  想……………….想……………….还是想。….跑去看会AV

回来一坐的时候发现有些用户密码，而且是他以前服务器的连接的FTP密码。

就考虑到留着密码可能管用

就开始导。。。可这是leapftp 。。这不是flashFxp坑爹啊！！！

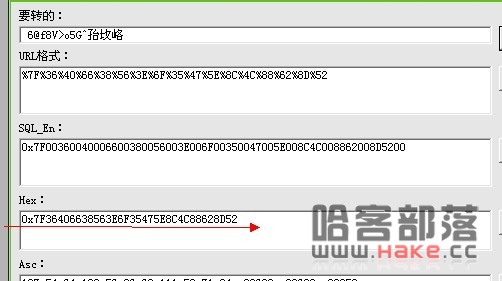
没办法。百度找一下方法、

方法如下

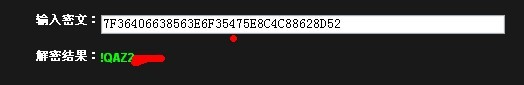
找到根目录的SITES.INI文件,Pass=后面的就是密文，转到HEX模式查看  
从506173733D开始到0D0A0D0A，这中间就是密码密文，复制出来本页解密  
存储结构：  
Pass=http://1v1.name  
506173733D7F7D49893F894985554F41445C446246508B4146414336833D7660824D7A4A0D0A0D0A  
得到7F7D49893F894985554F41445C446246508B4146414336833D7660824D7A4  
就是密文了,可以在本页解密。



加密的字符串取出来。用小葵转换



然后取0x后面的内容



然后解密成功，连续几个密码也解了。下面换思路。找他所有服务器。、开有FTP的端口的

128.2.2.1

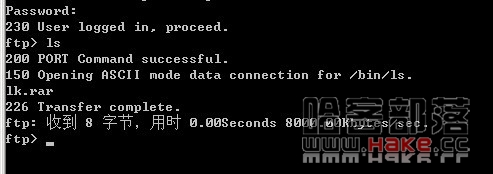
177.2.2.1

199.2.2.1

200.2.2.1

发现两台开了FTP服务。还是su6.3的

然后试一下账号密码。结果发现。几乎都是一样的。但只有一个压缩包



就一下压缩包 然后get下来。等了将近10分钟。有40M大，然后打开一看。这下高兴了。



数据库生成



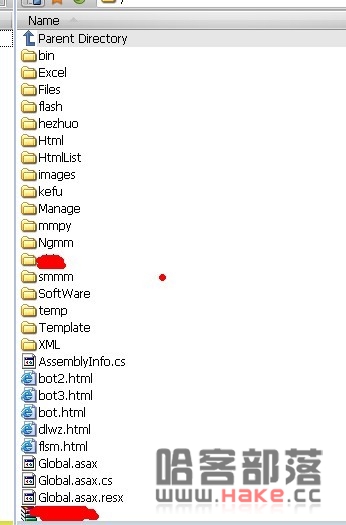
SA密码。

这叫送上门的把？

这下可把我高兴坏了。。。。。。然后兴匆匆的去连接，发现不开外端1433.这下的我彻底哭了。

有SA也木用。真尼玛的背！！！！

然后在乱试FTP密码。这下，真想抽自己。成功了。然后连上去发现。居然是 web目录。



只能无奈的完成了这次渗透

欢迎各位来到哈客。哈客欢迎您的到来

大牛勿喷。有错请指点！