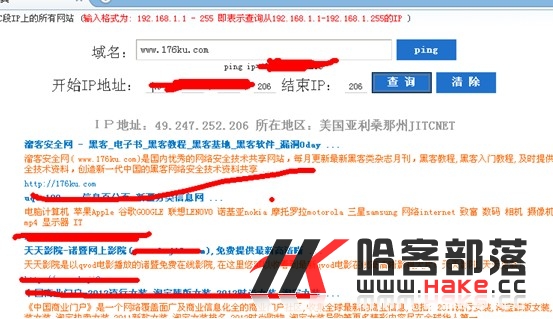
**文/图**

**作者:残剑**

**PS：该文章出稿时已联系站长。（转载请注重版权：From:哈客部落）**

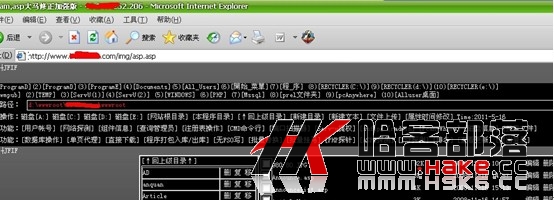
声明，此文章仅供技术交流,切勿恶意破坏别人站点.请人品有问题者自重！ 另外感谢一直旁边帮助我的某人。！(此人低调,就不公布名字了)

听说溜客是个很牛的站长开的,就想着来个友情检测.话说溜客原本是独立服务器的，但不知道为什么他最近搬去虚拟机了。

如图：  


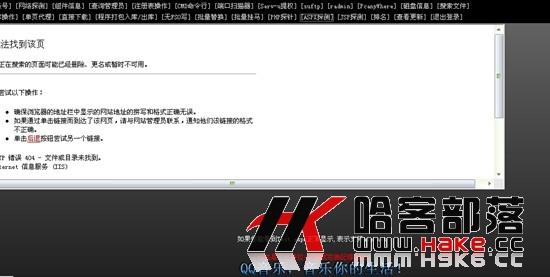
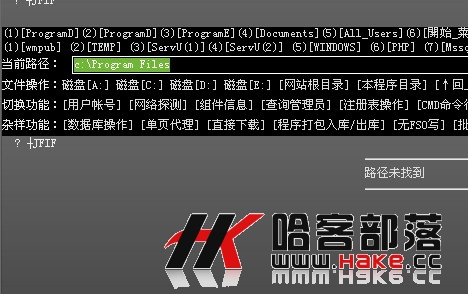
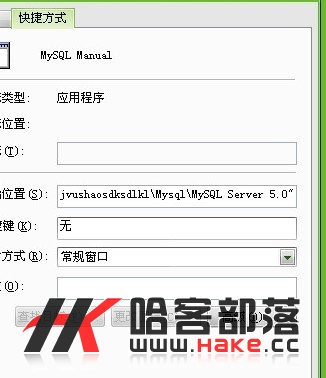
主站一般是木有漏洞的,不然早被人日了.所以接着旁站去了。我想大家都懂,那也是看运气啊,这样的站,不会是吃白饭的。旁吧旁吧~5分钟过了,10分钟过了…很苦恼，没日到一个SHELL~

随后一个一个仔细排查,遇到一个精良的系统,还是默认后台,直接拿下SHELL，这过程就不写出来了,我想大家都会…拿到了SHELL测试一下



还是星外的主机..并不支持.NET。很郁闷、也很悲剧…也没办法。继续翻翻敏感文件

连C盘可以的浏览都限制掉了.纠结！可是说几乎是没啥权限的..

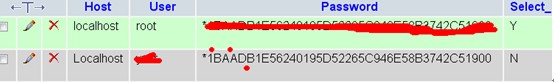
  
  
话说，是不是每个人的运气都可以这么好？  
  
能到找这目录  
，绝对的是人品问题,长相问题了！下载快捷方式，发现是在D:\cksjvushaosdksdlkl\Mysql\MySQL Server 5.0中  
  


人品大爆发。能就这样找到MYSQL目录。靠的还是细心..不过路径恶心了点

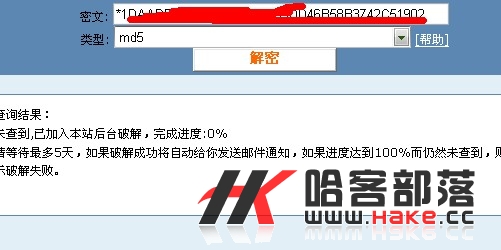


把data目录下的三个文件下载下来

然后自己架设MYSQL..有ROOT就可以提权了哇



至于，这能不能解是意料之中的

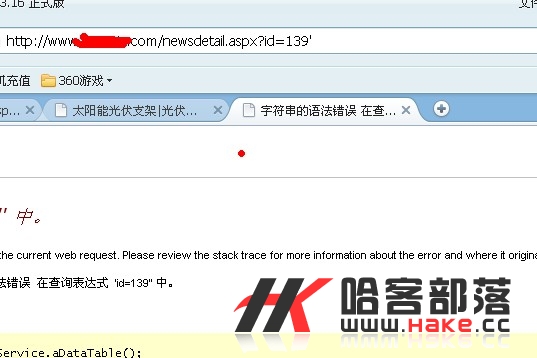


毕竟是虚拟机,那密码是有多长想都能想的出了。算了,放弃！

去看看这站点上有没有ASPX站，额?貌似这么多站就一个ASPX而已.很悲剧



想办法拿他SHELL。站点有注入



毕竟.NET与ASP方法不一样,不过就算是这样,数据库也是ACCESS而不是SQL ,让我感觉比较棘手了。

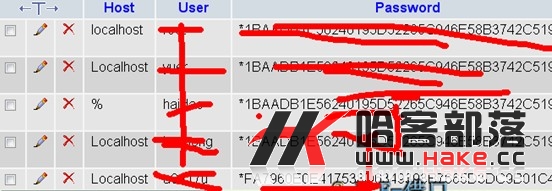
Order by语句查询字段数, 在3的时候反回正常



随后，由于这站是采用access的数据库,字典不够强大的原因在这站点上足足折腾了很久的时间。要么找不到表,要么找不到后台,最后人品爆发,社到了后台地址,但是由于网站太简陋了,只有一个精简过的eweb。其他没有任何可以下手的地方，最后还是以失败告终

过来一段时间，该搞的也搞了,该弄的也弄了,也没得到重要资料,思路到这里就卡住了。反正闲着也是闲着,无聊就只好翻翻其他的东西看了

突然想到,他不是有个论坛吗？忽然发现论坛的IP和主站竟然是一样的,那么也就是说数据库在这服务器上的几率有90%!!在mysql目录里翻了翻,下载了DATA数据里的东西.哇！这用户一大把一大把的



话说一下载下来我就纠结了!这可怎么找?有好几十个用户。不是要我一个个的试吧？算了,考验我耐心的时候到了…找啊找,发现一个很敏感的字眼Sq\_Liu\*\*\*\*

15.jpg

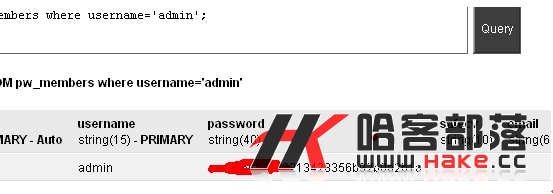
这感觉，像是抱着侥幸似的就拿去解密了.密码居然能解，你说淫荡不淫荡



接着就屁颠屁颠的拿着密码登录mysql去了



然后找表去。由于溜客用的是phpwind程序,而phpwind又是直接MD5加密的。我想,如果可以得到管理密码,这对于社工来说会是一个很大的突破



悲剧的密码.连Cmd5都无能为力,只好拜托有彩虹表的兄弟跑了一会。没想到的是,彩虹表也不能跑出来..看来站长是做好了完全的准备啊,弄了一个超级复杂密码.我想,做站长也挺难的,估计是这么复杂的密码要拿笔来记把?? 郁闷中…

先不管了，我们自己构造密码,然后进行md5加密。利用mysql语句,把原来的管理密码替换之.进后台拿SHELL试试,入侵PHPWIND的时候很多人傻到会被管理发现。不过我觉得进去之前大家先把日志部分记录下来，然后清理掉自己的IP。这样能使自己更安全一点,又不会引起管理的怀疑..否则数据库权限就不保了

进入后台,但是拿到SHELL..目前现有的漏洞貌似都补了,所以这后台也就暂时放弃了.先休息吧。都凌晨了~~

----一夜过去了,,,

早上刚睡醒就起来了.继续吧….

经过昨晚的奋斗，想了想。试探一下站长会不会去改自己MD5，我就故意把MD5的数字加了一个数字替换回去。过了一段时间.发现站长改密码了,拿去MD5解密依然不能解，果断发觉今天rp不是很好…

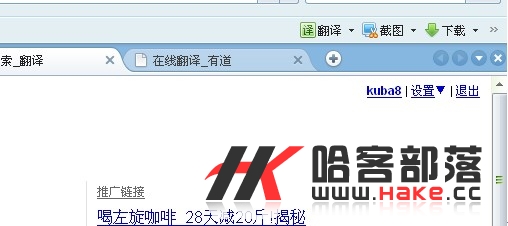
就这样过了几天……思路一点都没了,有点黔驴技尽了

没思路就和某牛在扯淡,他忽然和我说起溜客溜客啥的.他忽然说他有个文本是一年前社溜客的时候弄到的一个密码

这样把..可以选择信与不信吧,其实这密码我也很困扰..



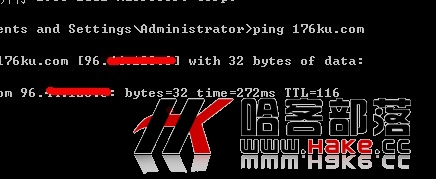
然后去百度找相关的密码资料



这密码居然还能登陆,话说这是一年前的密码啊！我感到很吃惊..简直就是奇迹

不过密码没什么用了，尝试大部分都无法登陆。也没思路了。又这样过了一天。。

第二天起来发现溜客换服务器了？



好好调查了一下。Idc居然是樱木花道大牛的.樱木可是俺很崇拜的一个人物哇

这站长该换的全都换了，让我更加没头绪.也不知道是不是被发现了,之后也在茫茫虚拟机中继续游荡…..没事做，就去看看他刚换的服务器有没有其他利用信息吧！

还好很快拿到了旁站的一个SHELL，但恶心的是,权限比上次的服务器还死..

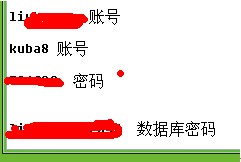


真无奈了。啥利用信息都没。毕竟是樱木做的安全。。

支持PHP，试试前几天的MYSQL密码看看



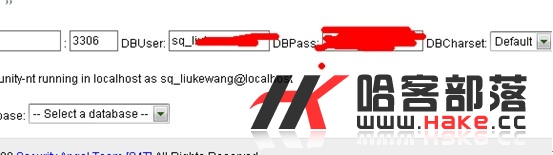
已经果断被改了。忽然才想起,研究一下他的密码规律吧



拿出这几天整理好的txt文本。就这几个密码有点很让人头疼,来随便组合一下把。账号和密码结合,密码和密码结合这样尝试

经过八组法功密码试炼法！哇里个擦. (这是我自创的神功,你们学不来的 哈哈)用旁站的SHELL试到了数据库！！！

这竟然是密码和账号的结合,,,这回他可悲剧了

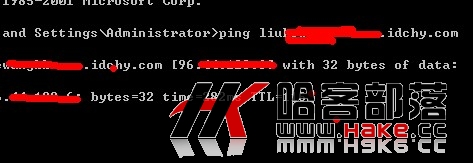


但试到密码有啥用呢??密码改了估计也拿不到SHELL,所以有这念头也放弃了之后去尝试一下统计的密码,其实大部分的密码都是一个经常用的.然后就很轻松的进去逛了逛。到处乱翻,,看到一个神秘的东西



怎么看都像是IDC.而且用户名与数据库相同,这样想的话，应该这就是IDC的FTP用户了？

然后PING一下。。确认确实是FTP



确实有点蹊跷,这会让我想起既然帐号和数据库用户是一样,那么密码会不会一样呢？去试一下.结果意料之外,居然能够成功登录了.以前也试过,但是FTP密码和这不一样。所以这感觉，纠结啊



同时沦陷论坛。只是用户和密码有点区别..换了一个组合尝试一下，通杀之~~



好了。文章写到这吧.此文章只是为了交流，请各种大牛勿笑，小弟拜谢