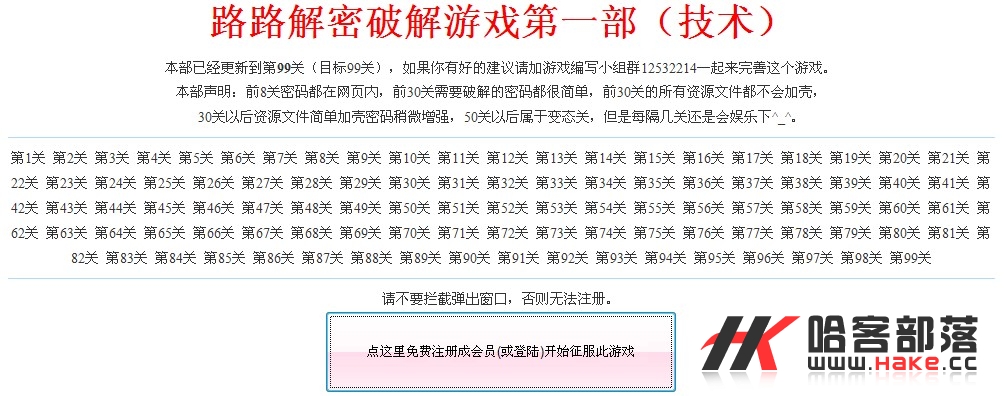
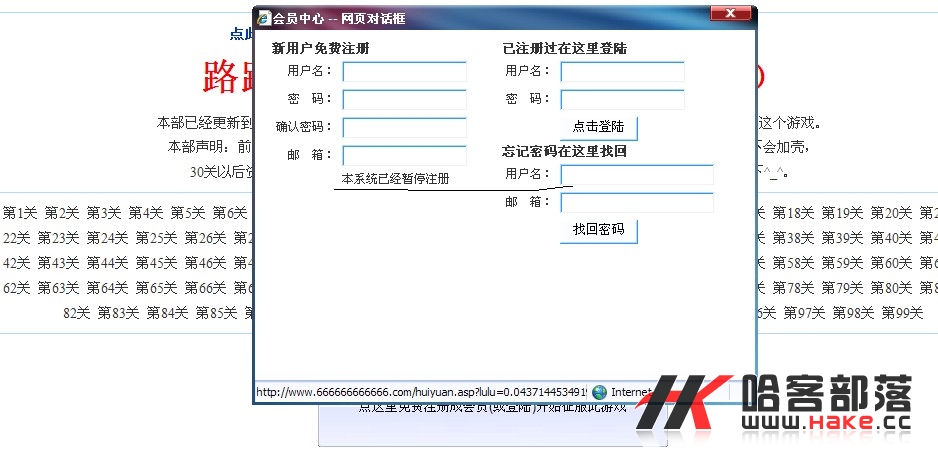
**文/图 残剑**

**话说前两天在情blog上看到了一些hakc game的游戏。当时也觉得无聊,就随便打开看了一下**

**点开链接一看。**



**这么多关卡?顿时被这个阵势怔住了。不过没关系,就当娱乐娱乐。反正也是闲着…..**

****

**蛋疼了一下。居然不能注册??**

**算了,就到主站去看看别的东西吧。**

**主站全是一些游戏各种的都有。技术类, 益智类,知识类, 娱乐类…等- -找了一个hack的游戏进去。**

****

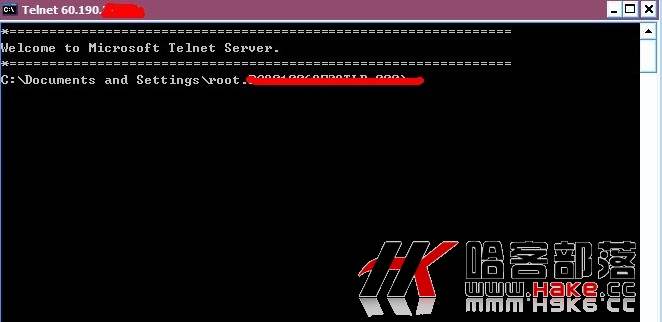
**顿时感觉这游戏咋这么….无语??**

**好吧。继续下去…**

**等到了第四关的时候**

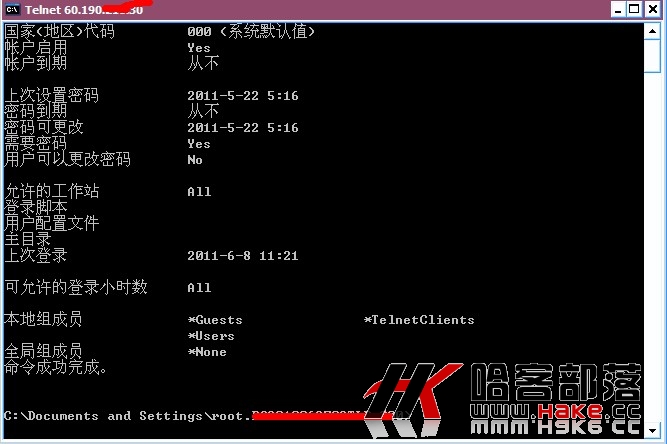
****

**他是要求我们入侵某个服务器。用telnet方式登入上去。不用说了,作者明摆着的意图就是说telnet有漏洞。接着拿着x-scan扫了一下服务器的telnet弱口令。果然存在…**

****

**看下dos界面,就有一种想要提权的心里。- -,,难道我是走火入魔了饿??**

**试了几个常用的命令。发现权限还不错。很宽松,,没有做什么特殊的设置。但仅仅是个guest权限**

****

**想想guest权限应该也很大,能做很多事了。本来是想上传一个提权工具上去的.但是百度死活找不到dos下上传文件的命令…够杯具的。**

**算了，先不管他,继续通关去吧……**

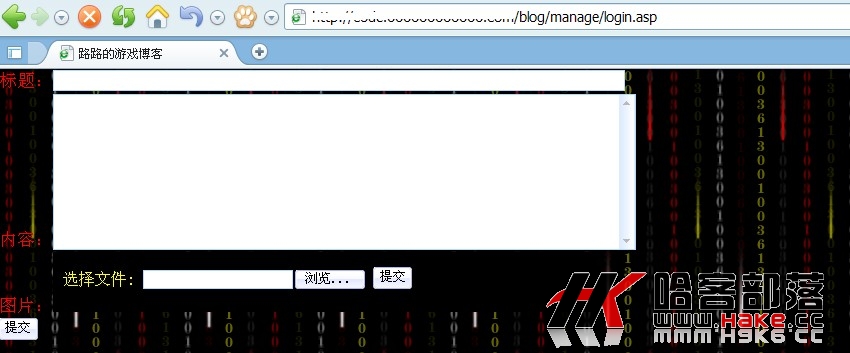
**从第9关开始就是入侵一个作者设定好的blog程序。**

****

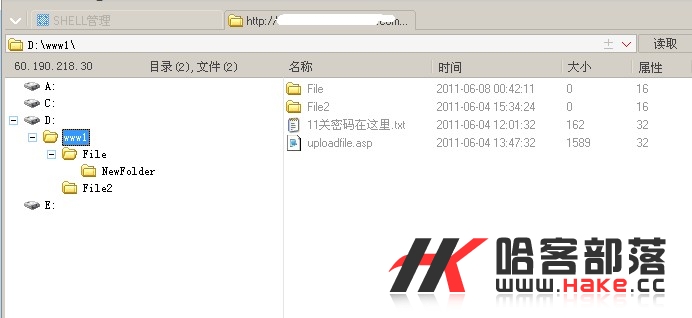
**后面几关也是一路顺风。但是当我看到最后一关的时候,我兴奋了..如图**

****

**这不是明摆着要送我们webshell么??还等什么??**

****

**程序没有对上传文件进行重命名处理,直接上传一个1.asp;1.jpg拿下。**

****

**传了个shell上去看了一下,虽然各个盘符不能浏览,aspx，php也不支持,服务器也没开1433,3306。万幸的是存在ws,看到这我就在想，他差不多该挂了吧。找了个可以写入的目录上传cmd。但是上传的时候出现 类型不匹配。这个我们可以无视他的,其实我们已经上传上去了。先systeminfo查看服务器的信息 并没有发现pr,烤肉的补丁号。**

****

**应该可以用pr秒杀。**

**上传pr执行C:\WINDOWS\Temp\pr.pdf "ipconfig",但是回显空白。试了试**

**C:\WINDOWS\Temp\pr.pdf "ipconfig" >> C:\WINDOWS\Temp\1.txt 访问1.txt提示输入超出了文件尾。看来确实是无回显的内容了。接着又试了试**

****

**看到了回显的内容。想想这种情况应该传个自定义路径的烤肉上去应该能解决。**

****

**还是提示错误。哎,,有点杯具了。又扔了几个ms的上去,还是无功而返..**

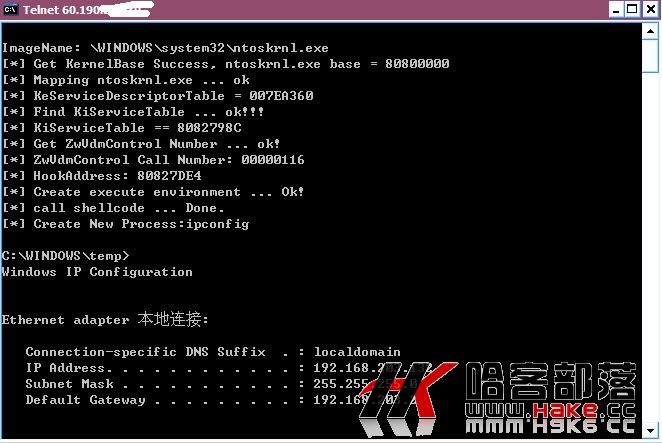
**突然灵光一现,想到不是还有一个guest权限的telnet用户嘛？哎,年纪大了,记性不好了,这个世界是00后的了..**

**跑题了,,我们继续**

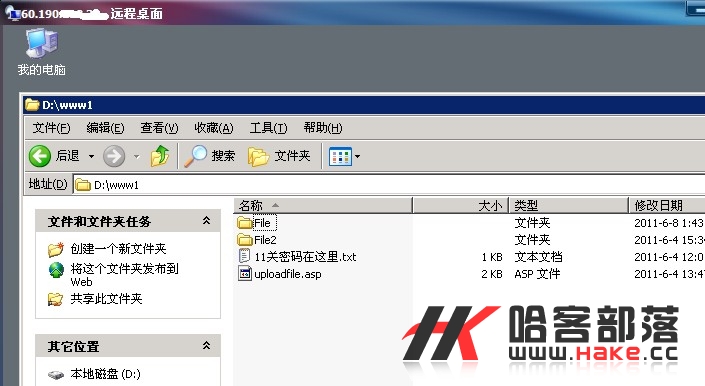
**再次telnet上服务器。Cd进去temp目录。用pr,烤肉执行命令。还是返回错误.搞到这就有点纠结了..难道这又是传说中的rp问题???**

**在关闭telnet前随手试了试ms10048提权。**

**居然执行成功了。**



**呵呵,既然是内网的。那就转发端口吧。转发成功后看了一下内网。居然是vmware,,杯具了。本来想渗透他主机的,想想算了。友情检测一下就好太过火就不道德了。呵呵,清理日志。通知管理..走人~~**

****