文/图

作者：过河的卒

昨晚已经很晚了，我们群群猪丢给我一个shell，让我看看，说他 cmd上不去，我就拿过来试一试。这台服务器是星外的，权限比较大，顺利找到一可读可写权限目录。

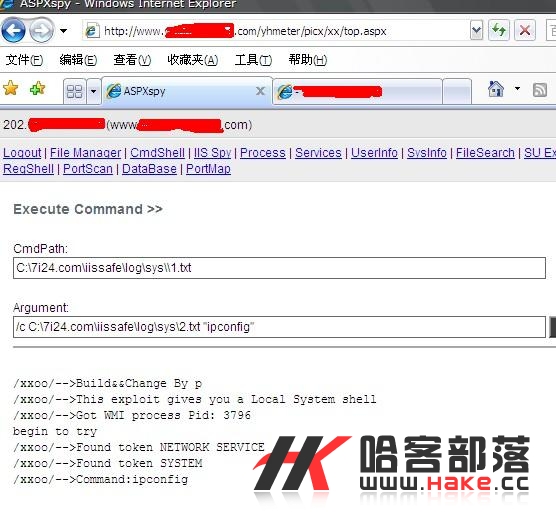


立即上传cmd.exe，因为我自己也需要尝试一下，果然是不能上传，我又改了cmd.com还是不能上传。我想会是文件名的问题么，如果这样，我把cmd.exe改为1.txt尝试上传，这次上传成功。



当然了，我们还要保证它的功能无损。一起在aspx马下看看结果。

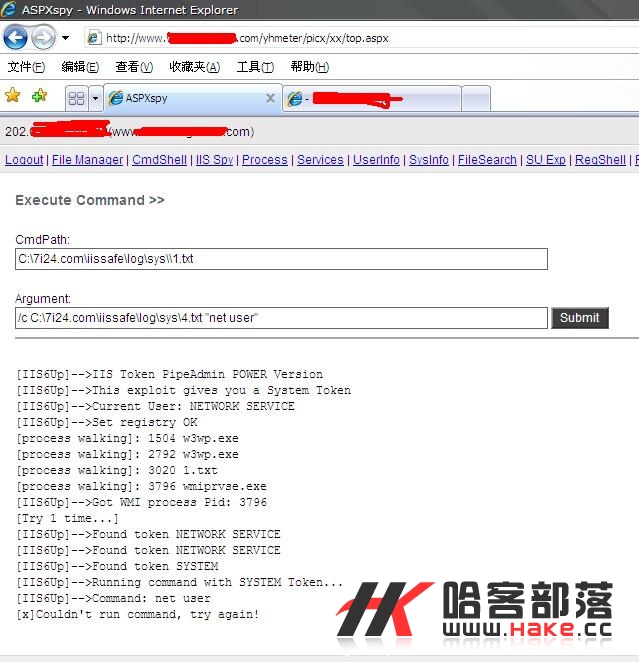
看得出他功能无损，星外提权，一般是利用vbs，今天我还是换种方法。我尝试一下pr，免参数pr之类的。2.txt是pr，3数pr，大家一起看结果。



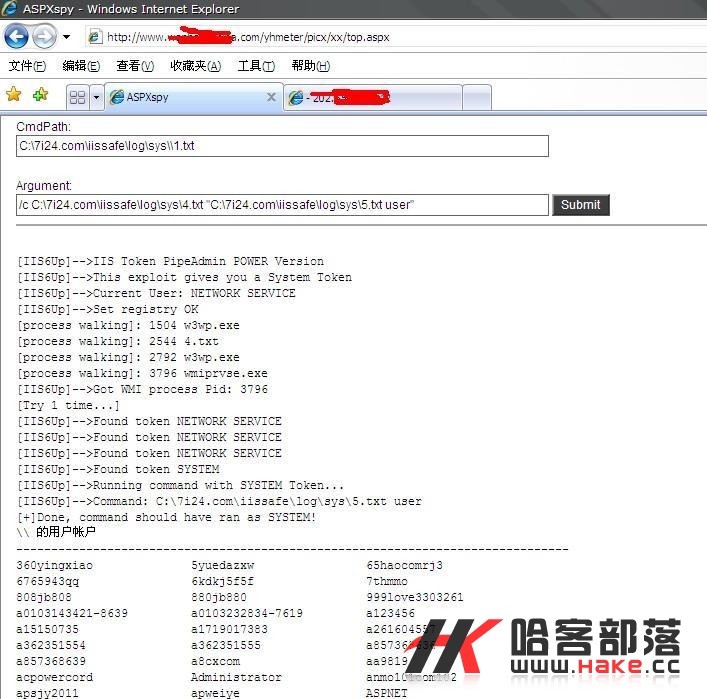
免参数pr也是一样的，pr失败，那么我们请出IIS6的一款0day工具，大家看图对比。



执行ipconfig成功，我们再来执行net user。



Net 执行失败，很明显是禁用了net，我们自己上传net或者net1，尝试添加用户。大家看我执行的命令，希望能给大家一些提示。



自此服务器已经沦陷，服务器截图就不放出来了，在服务器上看了安装有一流监控，主要是思路，此文章只做技术交流，大牛勿笑，小弟拜谢。