图/文

作者：人生

前几天，丫的把自己服务器不小心搞掉了，在这过程。了解到一个小方法，在这就公布给大家了。

  我发现开站的人，有一个缺陷就是，如果开了站就不把以前的站关了。这对站长的危害性有多大。

   废话不多说了。

目标是： xxx.com

我们下面了解一下，如图



该服务器之前是拿到权限的，可后来不小心掉了。 在他上面我发现有一个也是他开的站，但服务器并不在这里

PING他服务器上面的域名忽然发现有一个和这站域名曾经在这上面过。之前服务器掉了。没拿到想要的东西。只能继续渗透拿到想要的

如图



一台是58 一台是124 真是头疼。



不过那是曾经用的服务器，我们去翻翻之前的网站程序看看， 因为下载了新服务器很老以前的压缩包 其他也没打包。



是4月10号的。而且还有PHPMYADMIN 。估计大家都熟悉。

现在的站把PHPMYADMI删了。？杂办呢？

58上面还有他以前的站，58上面以前不是开着他的站么？嘿，估计你们也想到了。改HOST



我们把58和目标填进去，试改一下，看能不能访问？



、哈，这就是站长的病态了，我们可以利用旧信息去搞以前的服务器。我们看看能不能打开PHPMYADMIN

PS：对曾经用过的服务器如果存留着信息或者开启着，建议关掉。否则你会后悔的



  想想一下淫荡的表情，老服务器信息都是一模一样的

完全没改，旧信息肯定也没改。我们看一下ROOT能登陆不

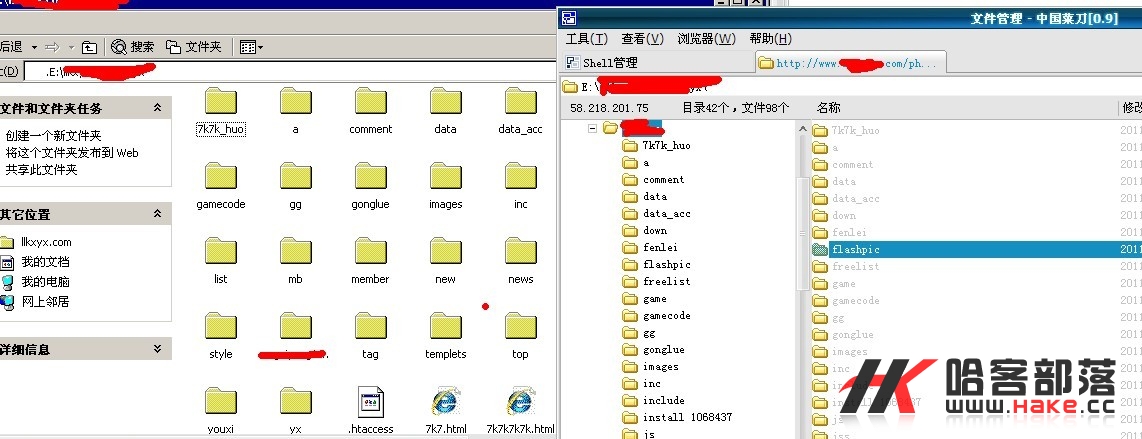


呵呵。一路畅通啊。 直接登陆



成功进入PHPMYADMIN 而且是ROOT。我想不用我说，大家都知道怎么拿SHELL了吧？ 如果实在不会百度一下，或者在论坛找一下MYSQL提权方法

SHELL到手 直接提权服务器



目标到手，。东西也拿到了。说明就到这了。 谢谢大家的观看

如此我们就可以知道，原本服务器的信息估计也是一样的吧，那我们取得HASH，反回拿那台就好了。但重点是HOST渗透重点，好了。 就这样吧

大牛勿笑，小菜只是总结经验