对某 90 后黑客联盟的 xxoo

Author : Desperado

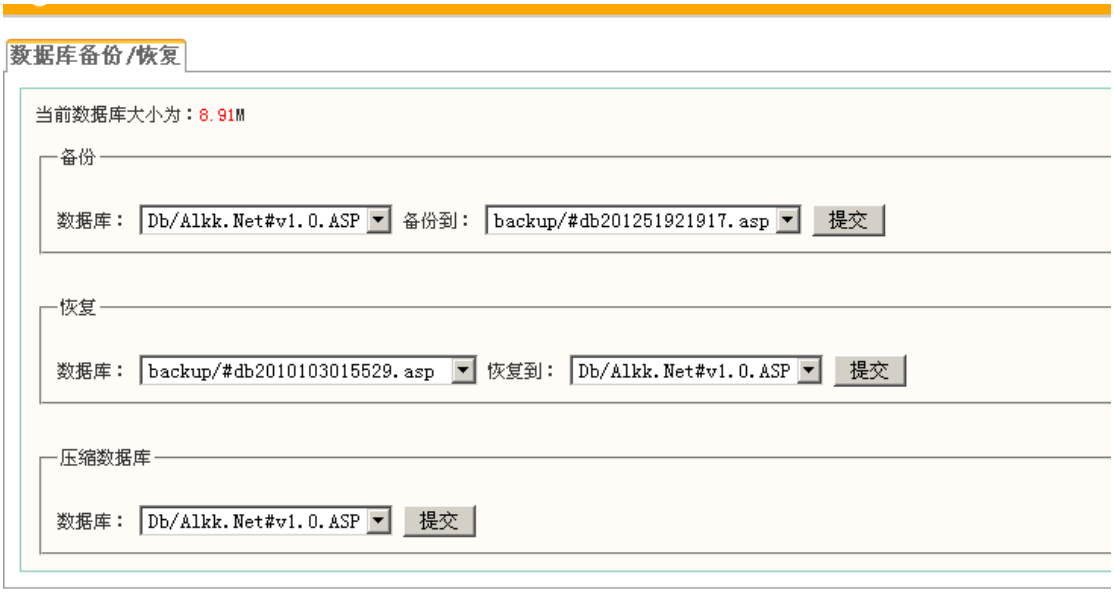
某日叫上 a11,随便挑个黑客站去 xxoo 下,过了会 a11 就发来了 www.90hsw.com 圈定目标后,我就展开了攻击~

Step 1

旁注出击:

由于是主站是 dz x2.0,我等小菜没有什么 oday, 因此直接选择旁注了.

一开始找到了个弱口令的站, http://www.szcuiwei.com/admin user:admin password:admin 进去,发现网站已经被一句话插得面目全非了,马上发给了 a11,我就回家吃饭了.回来后 a11 说拿不到 shell ,我自己也后台翻了起来,发现可以管理数据库，备份以及恢复.但是只能在选择框内选择,如图:

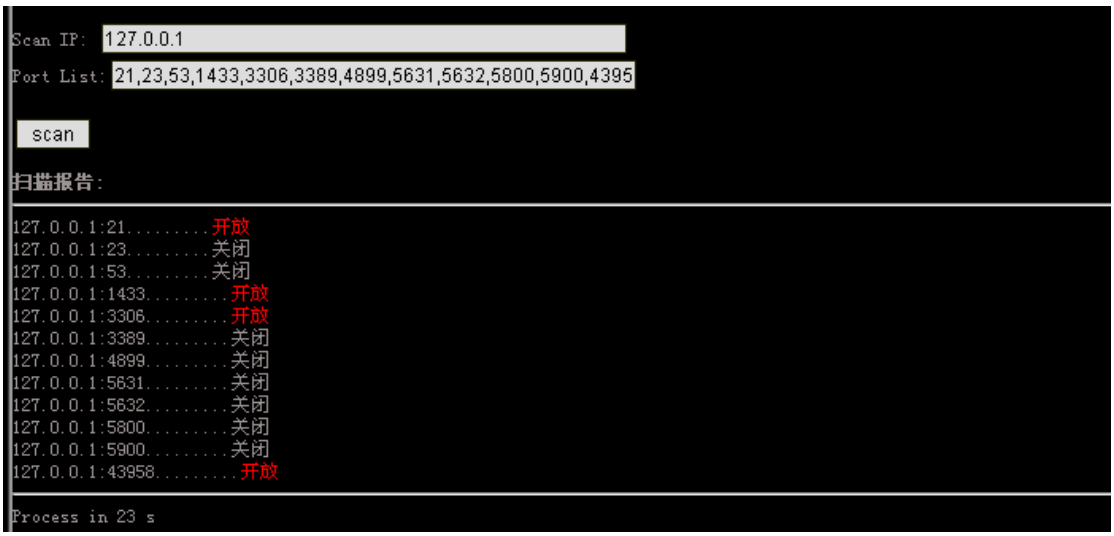


上传了 jpg,使用了 tamper data 来修改数据包的内容,ss 处填上自己上传的图片木马,tt 处填上木马的路径和名称.

不过恢复出来的马都显示错误,翻来覆去都不行(本地备份也试了),幸好后来 yaseng 牛无意中发现了一个前辈留下的一句话(我也不知道他怎么发现的),拿下了目标.

Step2 提权受挫

直接将拿到的 shell 扔给了 a11,查看了下组件 ws 是关着的支持 Php,不支持 aspx,php 的相关执行 cmd 命令的函数都被 kill 掉了,端口开放 如图:



还算乐观我们,1433,3306 和 43958 开着,翻了下数据库连接文件没得到想要的 sa 或者 db,mysql 和 serv_u 也就成了我们的突破口,a11 说试了 shell 自带的 serv_u 提权，由于 3389 关着,结果不知道,我试了那个 ftp 版的 serv_u 提权,结果同样令人失望的,

于是我戳到开始程序里发现了 serv_u 和 mysql 都躺着,下载了里面的文件,看了下属性

得到了他的路径(mysql 同理就不上图了),欢天喜地的输入路径->open,结果没有权限打开.

后来 A11 就去睡了.

Step 3 困难重重

我叫上 yaseng 继续,发现了这个服务器有的站是支持 aspx 的,找到了 ewebeditor,上传的模块好像被破坏掉了,由于是数据库是 asp 的,成功插了马.发现这个站是支持 aspx 的,还可以执行命令,那这个 90hsw 离大去之期应该不远了.

传了个 cmd 到 temp 目录,ver 了一下竟然是 xp:

Asp.net 权限比 asp 和 php 大,试着去打开 Mysql 和 serv_u 的路径,还是行不通,iis 探测一如既往得不成功,运行 systeminfo 没回显,pr 等杀器传上去都被 kill 了,我不懂免杀,也没办法,看了 cacls 一下想给存放网站的路径赋个权限结果也以失败告终,打开了目标站取了个图片名字想用 for 命令确定下目标站的路径也不行（for /r d:\www\ %i in (xx.jpg) do echo %i）.yaseng 也试了什么 iispwd 之类的也无功而返.改试得都试了.和 yaseng 讨论下基本宣布死刑了.想着 c 段太累了,准备放弃了.

Step 4 无奈 c 段

第二天把这个噩耗告诉了 a11,看他兴致依旧,就提出了 c 段吧,由于我还在上课.a11 瞄准了一台服务器,后来和 a11 cookie 注入进了 1 后台,经过一点波折传了一个小马。这个服务器不是一般的垃圾,大马传了很久都传不上,于是我传了个 aspx 的一句话,在 temp 目录上传 cmd,传死了都传不上去,什么东西都传不上去,又要放弃了?不行不行~

Step 5 峰回路转

最后我突然想起了论坛上不是有个帖子讲 dz 爆路径的么?我之前也收集了两个,试试吧.有了路径 copy move echo 都可以拿下目标.:

/source/function/function_connect.php

ucenter\control\admin\db.php

uc_server\control\admin\db.php

用第三条成功爆到路径

展开最后的致命一击,

Copy

d:\www\web\gzsmedu.com_cryQgbVddTKEyHP4wSVH\wwwroot\css\cool.aspx

D:\www\web\0817sc.com_EEF45SYA3RbQfTWLeMJi\wwwroot\sb.aspx

网站 B 卡 B 卡，过了很久终于返回 复制 1 个文件.Oh yeah.

顺利得拿下了目标,本次渗透也就告一段落了.

本文没什么亮点,都是各位前辈用烂了的方法,但也达到了目的,我想说的是,入侵渗透不是一条线,不是一条路,而是一个圈,只要你不放弃,兜兜转转之后,目标可能已经就在你脚下了.

Blog: www.arpman.com
欢迎各位来交流.