用电脑不求人系列之二十

GOTOP

防范黑客攻击

不求人

林东和 编著
樊小溪 改编

你知道 你的电脑
已经被 黑客攻击 了吗?
如何发现? 如何预防?

- 黑客攻击手段大曝光
- 剖析IIS系统大漏洞
- 防范E-mail炸弹攻击

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

用电脑不求人系列之二十

防范黑客攻击不求人

林东和　编著

樊小溪　改编

人民邮电出版社

图书在版编目(CIP)数据

防范黑客攻击不求人 / 林东和编著. —北京：人民邮电出版社，2002.5
（用电脑不求人系列；20）

ISBN 7-115-10076-4

I. 防… II. 林… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2002）第 019638 号

用电脑不求人系列之二十

防范黑客攻击不求人

◆ 编　　著　林东和
　改　　编　樊小溪
　责任编辑　俞　彬

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
　邮编　100061　电子函件　315@ptpress.com.cn
　网址　http://www.ptpress.com.cn
　读者热线　010-67180876
　北京汉魂图文设计有限公司制作
　北京顺义向阳胶印厂印刷
　新华书店总店北京发行所经销

◆ 开本：720×980　1/16
　印张：16.5
　字数：321 千字　　2002 年 5 月第 1 版
　印数：1-5 000 册　　2002 年 5 月北京第 1 次印刷

著作权合同登记　图字：01 - 2001 - 4824 号

ISBN 7-115-10076-4/TP・2760

定价：28.00 元

内容提要

本书是一本专门探讨防范黑客攻击的书籍，全书使用简单的图例及步骤，按部就班、循序渐进地指导你学会如何防范黑客攻击。

第一章介绍黑客攻击的基本概念，第二章介绍 IIS Unicode 攻击流程，第三章讲解 Unicode 攻击伎俩，第四章介绍上传木马攻击法，第五章介绍 Outlook Express 木马攻击伎俩，第六章介绍 Outlook DOS 攻击法，第七章介绍 E-mail 窗口炸弹，第八章是特洛伊木马的详细列表，第九章介绍系统漏洞修补大法，第十章是黑客攻击的实例解说。

本书内容简明扼要、通俗易懂，适合对网络安全知识感兴趣的电脑用户阅读，也可供网络管理员、系统维护人员、网络用户及大专院校相关专业师生学习参考。

丛书前言

电脑的魅力不但在于其高效和用于娱乐，更重要的是它始终体现着我们这个时代的脉搏。电脑技术的发展日新月异，硬件在不断升级换代，软件版本也在不断更新。这固然给用户带来了欣喜，但同时也给用户造成了压力——必须不断地学习和实践。

电脑作为一种工具，它最鲜明的特点就是用户可以自己组装、更新各种部件，使自己的电脑不断升级，以满足需要。在成千上万的电脑品牌后面，有数不清的电脑部件生产厂商在提供不同类型的零配件。当然，您在看到有更新型的部件之后，也不妨自己动手进行更换，使电脑更好地工作。但是自己动手，问题就来了。例如：如何预防、减少硬件故障的发生；在硬件故障发生后如何及时排除和修复；如何安装、升级电脑硬件；如何保证电脑可靠运行而且能更好地发挥作用等等，这些已成为众多计算机用户和广大专业维修人员十分关注的问题。《用电脑不求人系列》丛书即可帮助读者解决这些问题。这套系列丛书的最新书目如下：

- 《选用主机板不求人(第二版)》
- 《升级电脑不求人》
- 《电脑死机不求人》
- 《电脑优化不求人》
- 《防范黑客不求人》
- 《Windows 系统急救不求人》
- 《防范黑客秘籍不求人》
- 《急救硬盘不求人》
- 《VCD 光盘刻录不求人》
- 《架设网络不求人》
- 《设置 BIOS 不求人》
- 《实战黑客不求人》
- 《电脑多重启动不求人》
- 《防范黑客攻击不求人》

组织出版这套丛书的目的是为了深入浅出地介绍各种硬件设备的规格、类型及其安装、升级的知识，并通过简单明了的图例和实际操作步骤的介绍，循序渐进地引导读者掌握各种硬件的使用方法。鉴于许多电脑用户和大中专院校学生虽具有一定的电脑基础知识，但对于机器内部各种部件到底是什么模样并不很清楚，这套丛书中提供了大量实物照片，可以帮助读者增加感性认识。另外，每章的最后一节是“问题与解答”，它可以为读者解答疑难问题，巩固所学的知识。

我们力求使本丛书突出实用性强的特点，以适合广大电脑爱好者进一步学习电脑知识的需求，帮助广大读者提高使用、维修电脑的能力。

我们希望这套丛书能成为用户使用电脑过程中的好朋友。

编者

2002 年 2 月

目 录

第一章 概　述

1-1 引言

IIS Server（Internet Information Server）系统是微软公司主推的网页服务器系统，目前其市场的占有率正呈上升趋势。

然而，IIS Server 服务器有一个严重的 Unicode 漏洞，黑客可以经由此漏洞轻易地攻击 IIS Server 服务器系统，更能够任意地更改网页内容。

本书将要介绍这个 Unicode“惊世大漏洞”，并揭开黑客利用 Unicode 漏洞攻击的伎俩。

除此之外，本书还介绍了 Outlook 及 Outlook Express 的几个致命漏洞，这些漏洞使黑客可以利用 E-mail 来攻击他人。下面对本书的具体内容做一概要介绍。

1-2 IISUnicode 攻击流程

IIS 是微软所推出的一套网络服务器软件（见图 1-1），准备和 Apache 一较长短。

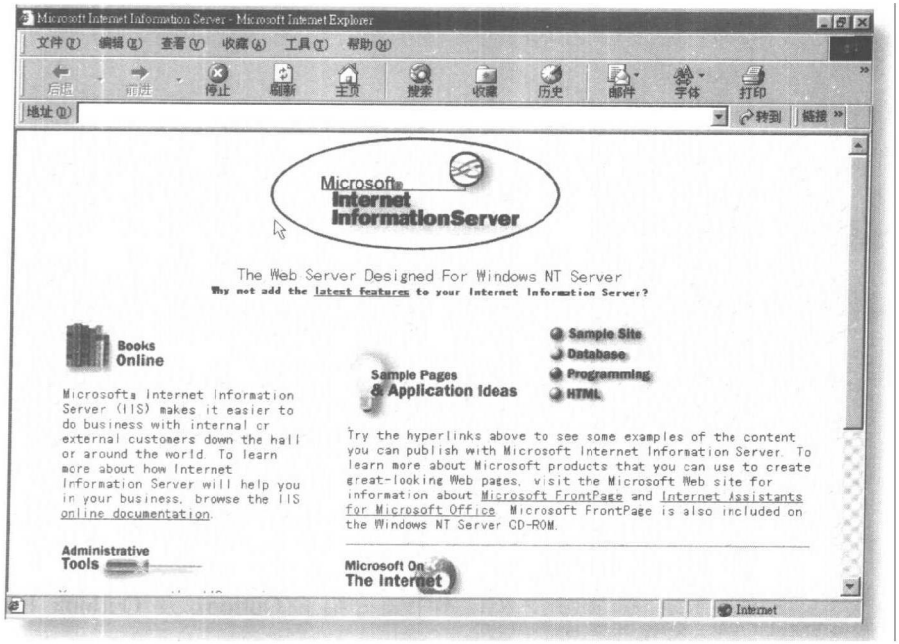


图 1-1

Unicode 是 IIS 系统的一种编码方式，当你打入“%c1%9c”字符串时，IIS 会将它编码成“\”，也就是反斜线字符。

于是，黑客利用此 Unicode 漏洞（见图 1-2）突破 IIS Server 目录的限制，进而入侵 IIS Server 系统。

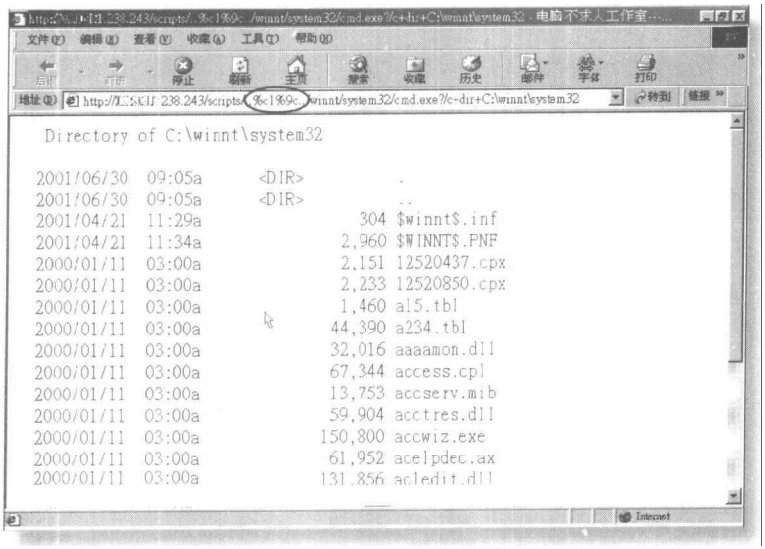
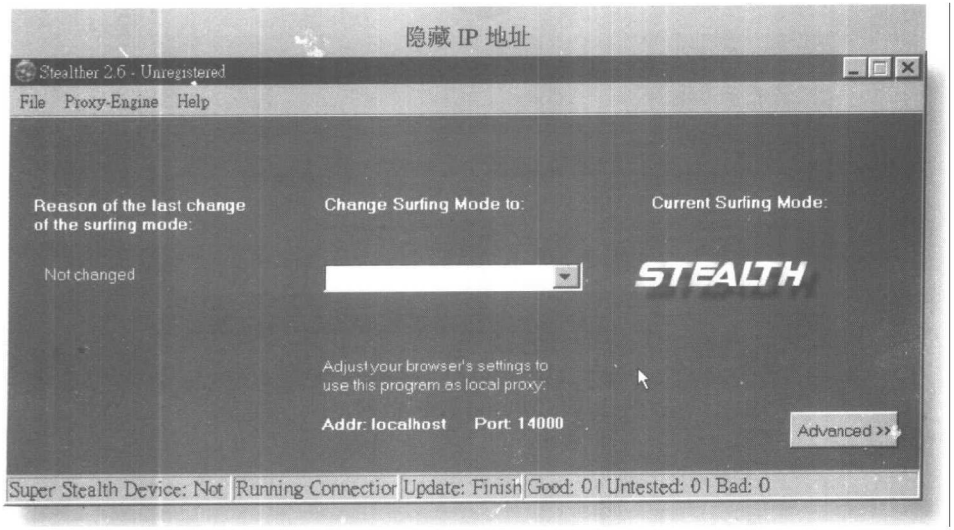
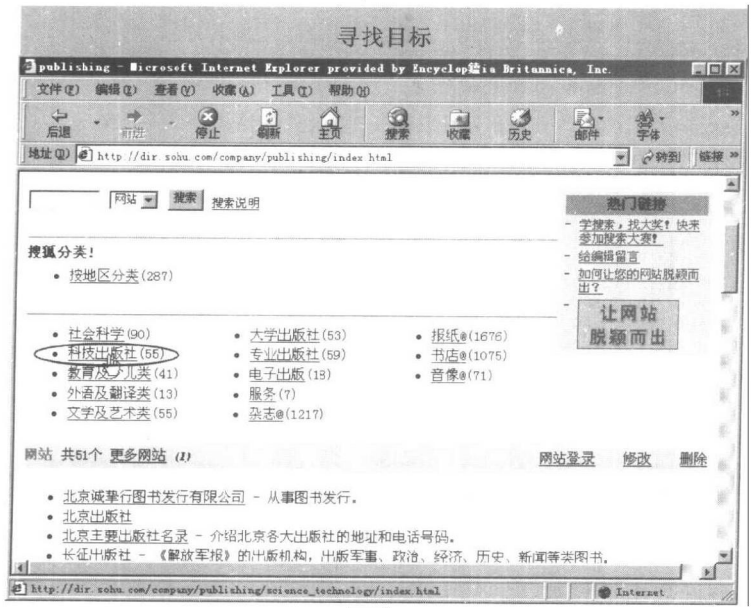


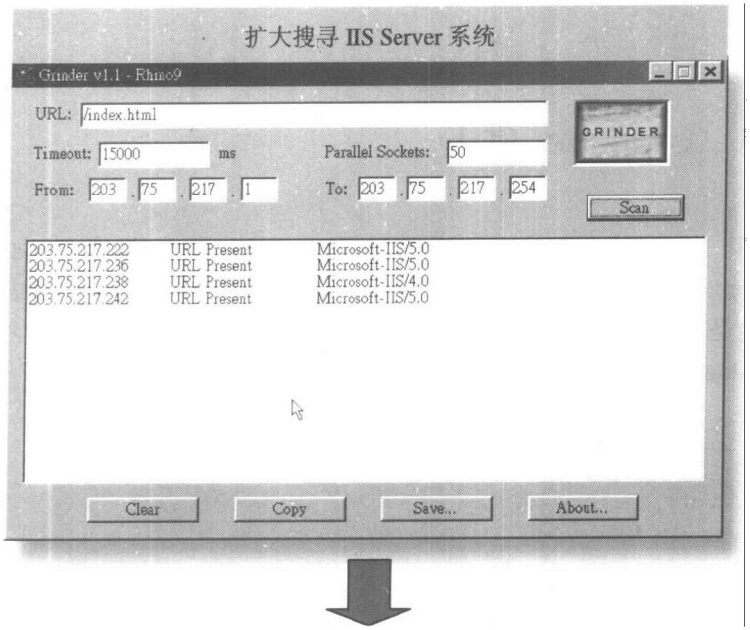
图 1-2

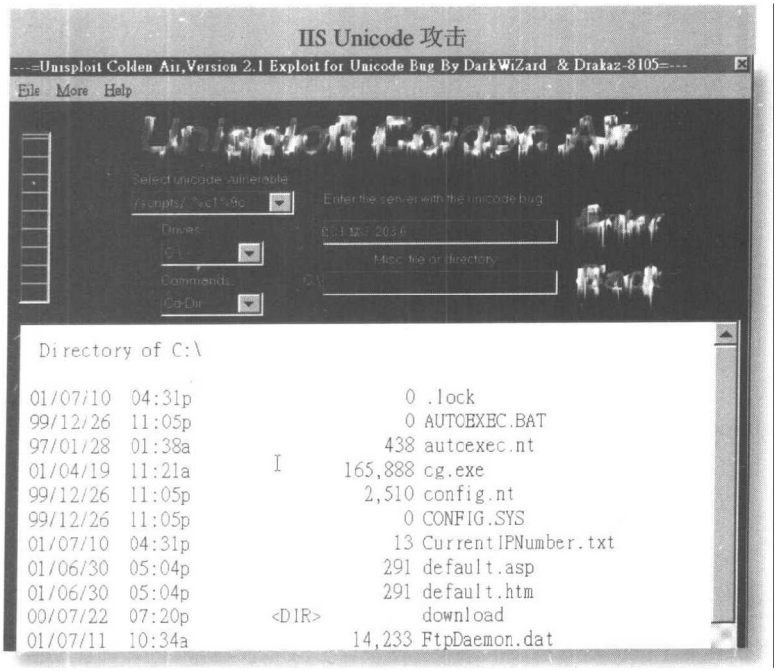
IISUnicode 攻击流程如下。




寻找目标
publishing - Microsoft Internet Explorer provided by Encyclopaedia Britannica, Inc.
http://dir.sohu.com/company/publishing/index.html
搜索
搜索说明
热门链接
搜狐分类!
按地区分类(287)
社会科学(90)
科技出版社(56)
教育及少儿类(41)
外语及翻译类(13)
文学及艺术类(55)
大学出版社(53)
专业出版社(59)
电子出版(13)
服务(7)
杂志@(1217)
报纸@(1676)
书店@(1075)
音像@(71)
让网站脱颖而出
网站 共51个 更多网站 (1)
网站登录
修改
删除
北京诚挚行图书发行有限公司 - 从事图书发行。
北京出版社
北京主要出版社名录 - 介绍北京各大出版社的地址和电话号码。
长征出版社 - 《解放军报》的出版机构，出版军事、政治、经济、历史、新闻等类图书。
http://dir.sohu.com/company/publishing/science_technology/index.html
Internet


确认 IIS Server 系统
IntelliTamper
File Help
Address http://www.gotop.com.tw/
Information
Now scanning server at 203.75.217.238 on port 80...
Informations on domain "www.gotop.com.tw":
Server software : Microsoft-IIS/4.0
Server time : Wed, 11 Jul 2001 02:35:23 GMT
Unable to connect to server, tyng again.
Unable to connect to server, tyng again.
Unable to connect to server, tyng again.
Connections status
GET "/dnload/_index_defaultpage.html"...
GET "/group/_index_defaultpage.html"...
GET "/Movie1.swf"...
GET "/sec2/img/sec2-news.swf"...
GET "/sec2/index4.htm"...
GET "/sec4/booking.asp"...
GET "/sec4/Demo/firmware.html"...
GET "/sec4/Demo/help100_body.html"...
Web
www.gotop.com.tw
group
img
sec1
sec2
img
sec3
img
sec4
Demo
img
sec5
img
project
sec6
Name
Size
Last modif
image004.gif - KB
image007.gif - KB
image008.gif - KB
image009.gif - KB
image010.gif - KB
image012.gif - KB
image013.gif - KB
image017.gif - KB
Extra links in selected file
开始
hacker5
HALO Des...
IntelliTamper
AM 10:29





有关 IIS Unicode 攻击流程的详情，请参考第二章的详细介绍。

1-3 Unicode 攻击

黑客利用 IIS Unicode 攻击流程找到攻击的目标后，就会进行 Unicode 攻击了。

下面笔者介绍一套功能强大的 Unicode 攻击软件——Unisploit-Colden Air（见图 1-3），这是一套由 DarkWizard 设计的 Unicode 漏洞攻击软件，黑客只要使用 Unisploit-Colden Air 软件，攻击 IIS Server 系统就变成一件很简单的事。

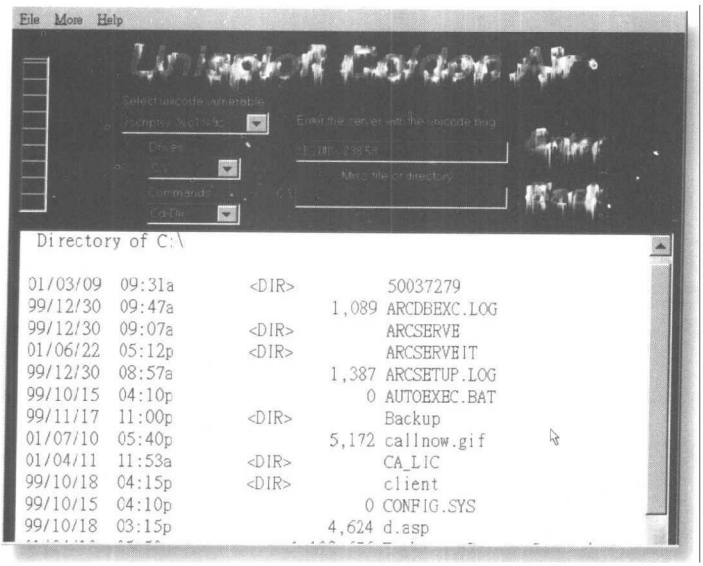


图 1-3

有关 Unicode 攻击详情，请参考第二章的详尽介绍。

1-4 上传木马攻击

一旦用 Unisploit-Colden Air 找到有 Unicode 漏洞的 IIS Server 系统之后，黑客

为了要完全控制该 IIS Server，最好的方法就是上传木马到该 IIS Server 中。

黑客为了要完全控制 IIS Server 系统，往往会使用类似 Khe Snah 木马（见图 1-4）类型的程序，该程序操作界面类似“Windows 资源管理器”，而且可以进一步攻击局域网络系统。

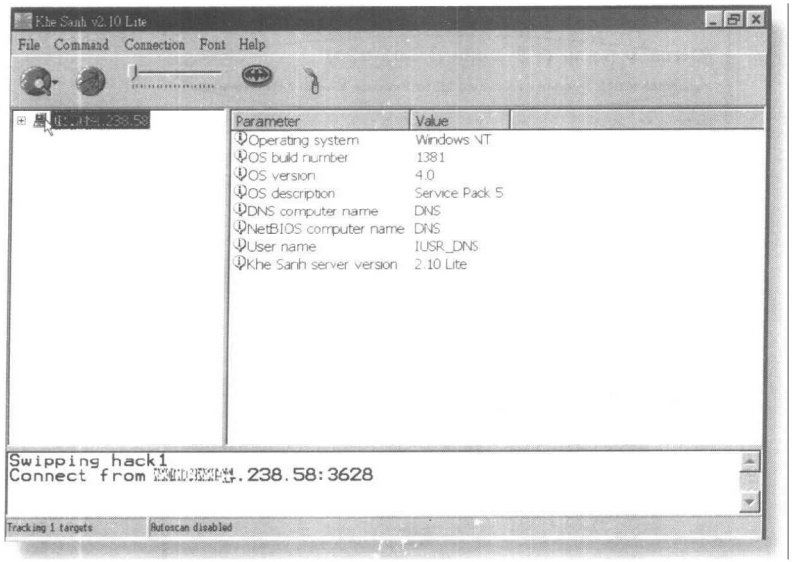


图 1-4

有关上传木马攻击详情，请参考第四章的攻击程序说明。

1-5 Outlook Express 木马攻击

Outlook Express 木马攻击是利用 Outlook Express 的 MS01-020 的“Incorrect MIME Header Can Cause IE to Execute E-mail Attachment”（不正确的 MIME 报头导致 IE 运行邮件附件）漏洞（见图 1-5）来攻击，这个漏洞可以让黑客利用一封夹带木马程序的 HTML 格式的 E-mail 来攻击他人，当被黑者收到这封攻击邮件后就会“立即”激活木马程序。

笔者模拟黑客制作了一个 Outlook Express 木马攻击邮件（见图 1-6），让你可以亲身体验一下。

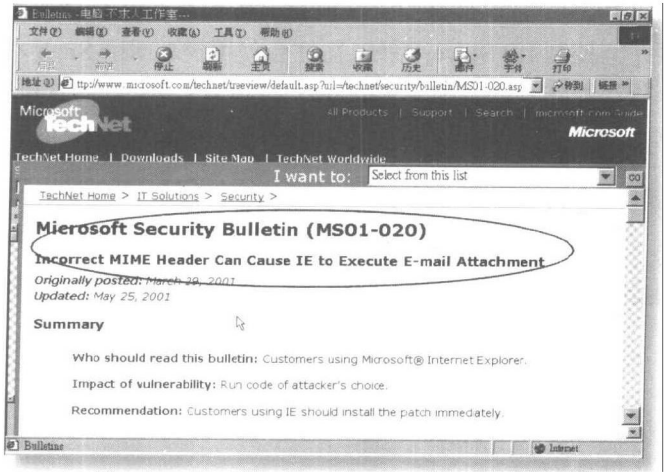


图 1-5

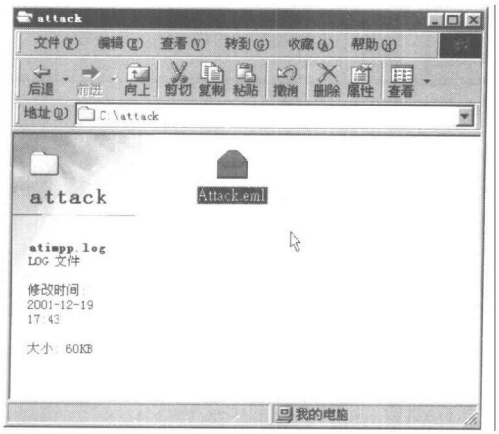


图 1-6

有关 Outlook Express 木马攻击详情，请参考第五章的详细解说。

1-6 Outlook DoS 攻击

Outlook DoS 攻击是利用 Outlook 的 MS00-043 的 Malformed E-mail Header 漏洞（见图 1-7）来攻击。