

Self-Teaching Guides

Self-Teaching Guides

无师自通+11

黑客攻防超简单

启典文化 编著

```
Module1Option ExplicitSub()DimAsLongDimAsIntegerDimAsIntegerDimAs  
StringDim i As IntegerIf ActiveCell.Value = "" ThenActiveCell.Value = 1End  
IfActiveCell.ValueWorksheets.CountActiveCell.AddressFor i = 2 ToWorksheets(i).  
ActivateRange().Value =Next-End SubSub 2()DimAs LongDimAs IntegerDim  
As IntegerDim As IntegerDim As StringDim As StringDim As WorksheetDim i  
As IntegerIf ActiveCell.Value = "" ThenActiveCell.Value = 1End IfActiveCell.  
ValueWorksheets.CountActiveSheet.ActiveCell.AddressFor EachIn  
Worksheetsi = i + 1If.NameWorksheets(i) ActivateRange()  
Next End SubModule1Option ExplicitDimAs LongDim As IntegerDim As Integer  
Dim As IntegerDim As IntegerDim As StringDim As StringDim As Worksheet =
```



攻击招式 破解有方 / 系统防护 全程无忧 / 信息安全 轻松搞定

```

IfNextApplication.CutCopyMode = FalseEnd SubModule1Option ExplicitSub
()Dim i As IntegerDim As Integer = InputBox("")For i = 1 To Sheets Copy
before:=Sheets(1) ActiveSheet.Name = Right("00" & Worksheets.Count - 1, 3)
Next i Sheets Activate End SubSubDim i As IntegerSheets.Add Before:=Sheets(1)
ActiveSheet.Name = "%"Range("A:A").NumberFormat = "@<For i = 2 To Sheets.
CountCells(i - 1, 1).Value = Sheets(i).NameIf Application.Version >=
- 1, 1).SetPhoneticEnd IfNext iRange("A1").Sort Key1:=Range("A
Sheets.Count - 1Sheets(Sheets( "%").Cells(i, 1).Value) _ Move
Next iApplication.DisplayAlerts = FalseApplication.Display
SubName <>ThenActiveSheet.PasteEnd IfNextApplica

```



买书即可参加**抽奖**活动

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

10台iPad mini等你拿 下一个时尚达人就是你!

Self-Teaching Guides

无师自通+11

——黑客攻防超简单

启典文化 编著

```
Module1Option ExplicitSub()DimAsLongDimAsIntegerDimAsIntegerDimAsStringDim i As IntegerIf ActiveCell.Value = "" ThenActiveCell.Value = 1End IfActiveCell.ValueWorksheets.CountActiveCell.AddressFor i = 2 ToWorksheets(i).ActivateRange().Value =Next End SubSub 2( DimAs LongDimAs IntegerDimAs IntegerDimAs IntegerDimAs StringDimAs StringDimAs WorksheetDim i As IntegerIf ActiveCell.Value = "" ThenActiveCell.Value = 1End IfActiveCell.ValueWorksheets.CountActiveSheet.NameActiveCell.AddressFor EachInWorksheetsi = i + 1IfName ThenEnd IfNextFor i = Worksheets(i).ActivateRange()Next End SubModule1Option ExplicitSubDimAs StringDimAs Worksheet =
```

攻击招式 破解有方 / 系统防护 全程无忧 / 信息安全 轻松搞定

```
IfNextApplication.CutCopyMode = FalseEnd SubModule1Option ExplicitSub()  
(Dim i As IntegerDimAs Integer = InputBox(" ")For i = 1 To Sheets Copy  
before:=Sheets(1).ActiveSheet.Name = Right("00", 3 - Worksheets.Count - 1, 3)  
Next i Sheets ActivateEnd SubSub Add Before:=Sheets(1).ActiveSheet.Name = "%R"  
"@For i = 2 To Sheets.CountCells(i - 1, 1).Value = Cells(i).ValueApplication.Version >= 10.0.0.0  
- 1, 1).SetPhoneticEnd IfNext IfRange("A1").Sort Key:=Range("A1")Worksheets.Count - 1Sheets(Sheets("%").Cells(i, 1).Value) Move  
Next iApplication.DisplayAlerts = FalseApplication.DisplayAlerts = False  
SubName <>The iActiveSheet.PasteEnd IfNext Application
```



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书以 Windows 7 操作系统为平台,力求用简练的语言介绍黑客入侵和防范的相关知识。

本书共 8 章,从对电脑黑客的基本认识开始,通过对黑客工具的介绍和各种黑客攻击方式与手段的认识,全面讲解黑客攻防中的点点滴滴。通过这些知识,不仅能够帮助初学者学习电脑安全及黑客攻防的相关知识,还能够让初学者了解黑客入侵的方式,以及解决被攻击的问题和隐患。

本书内容简单实用、通俗易懂,版式清晰、简洁,相信能帮助读者快速而灵活地掌握黑客攻防的相关知识。

本书适用于初中级的电脑维护人员、IT 从业人员学习,以及对黑客攻防和安全维护感兴趣的读者自学参考,也可作为大中专院校和各种电脑培训班的学习教材。

图书在版编目(CIP)数据

黑客攻防超简单 / 启典文化编著. — 北京: 中国铁道出版社, 2013. 7

(无师自通)

ISBN 978-7-113-16490-4

I. ①黑… II. ①启… III. ①计算机网络—安全技术
IV. ①TP393.08

中国版本图书馆CIP数据核字(2013)第094239号

书 名: 无师自通——黑客攻防超简单
作 者: 启典文化 编著

策 划: 张亚慧
责任编辑: 吴媛媛
封面设计: 多宝格
责任印制: 赵星辰

读者热线: 010-63560056
编辑助理: 刘建玮

出版发行: 中国铁道出版社(北京市西城区右安门西街8号 100054)

印 刷: 中国铁道出版社印刷厂

版 次: 2013 年 7 月第 1 版 2013 年 7 月第 1 次印刷

开 本: 880 mm×1 230 mm 1/32 印张: 8 字数: 232 千

书 号: ISBN 978-7-113-16490-4

定 价: 29.00 元(附赠光盘)

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社发行部联系调换。

前言

FOREWORD



Why——编写原因

随着互联网技术的不断发展，网络新功能不断涌现，使信息的交流更加高效、快捷，网络已成为人们生活、工作中必不可少的一部分。与此同时，网络中出现了一群被称为“黑客”的人物，他们以恶作剧、炫耀、报复、经济利益等目的攻击网络中的电脑，使网络信息安全问题成为电脑用户的一大忧患。

为了使用户更好地预防黑客攻击，需要知己知彼，在了解和认识黑客攻击的方式后，为电脑设置“一道门”，保护用户的电脑和信息安全。因此，我们特别编写了这本清晰、简单、实用的《无师自通——黑客攻防超简单》，力求用简练的语言，教会电脑用户认识黑客攻击，防备黑客攻击。

What——本书内容

本书共8章，涵盖了黑客的概述，信息的搜集、嗅探与扫描，基于系统漏洞的入侵与防范，远程控制技术，基于木马的入侵与防范，平时上网的黑客攻击与防范，安全防范黑客入侵，信息的隐藏与后门清理等8个方面的内容。

各部分的具体内容如下。

黑客的概述

第一章讲述了黑客的基本知识，揭秘黑客使用的一些常用命令，让用户认识黑客究竟是什么、黑客是怎样操控网络的等知识。

信息的搜集、嗅探与扫描

黑客获得的信息越多，攻击就会越容易，对于用户来说，了解自己的弱点才能防患于未然，第二章介绍了一些常用的信息搜集、嗅探与扫描的方法和工具。



基于系统漏洞的入侵与防范

黑客会利用系统存在的漏洞进行攻击，用户也要了解漏洞并进行安全防范，第三章介绍了基于漏洞的攻防和常见的密码破解。

远程控制技术

黑客可通过远程控制技术控制用户电脑，从而获取信息并进行远程修改等，第四章讲述了通过认证、远程修改注册表等入侵方式以及对应的安全防范。

基于木马的入侵与防范

木马有着强大的控制力和破坏性，能窥探重要信息、控制操作系统等，是黑客攻击的重要手段。第五章介绍了木马的基本知识，使用户了解木马的攻击原理以及木马的清除方法，进而安全防范木马入侵。

平时上网的黑客攻击与防范

用户上网进行聊天、购物、收发电子邮件、浏览网页等应用，成为黑客最喜欢的攻击对象。第六章以QQ、电子邮件、浏览器等为例，介绍黑客的攻击方式与安全防范。

安全防范黑客入侵

保证用户电脑的网络安全，要对其进行一系列安全设置。第七章通过介绍IP地址、端口的设置，系统安全处理等，让用户了解安全防范黑客入侵的具体方法。

信息隐藏与后门清理

黑客要想方设法地隐藏在服务器上留下的入侵信息，让自己的攻击不会被用户发现，第八章介绍了黑客攻击的信息隐藏技术和后门清理的方法。

How——怎么学习

► 用直观的标题介绍知识

本书精选的知识点都是比较实用的内容，通过从直观的标题中就可以清楚地了解知识点的用处，有的知识点中还讲到了几种方式或内容，读者可以根据需求进行查询学习。

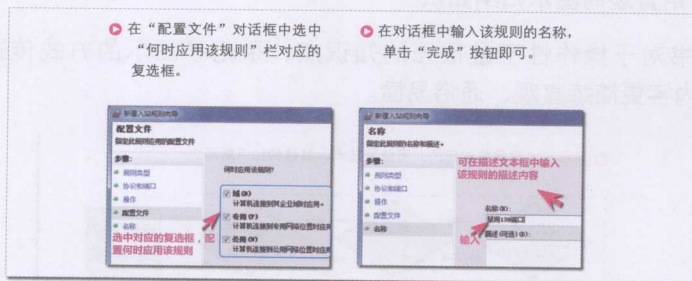
第二节 黑客 与IP地址

03 用命令查看本机IP地址

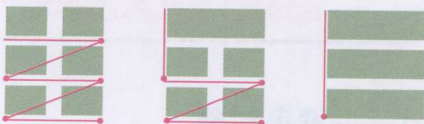
用命令查看本机的IP地址，需要略懂DOS命令，在命令提示符下输入简单的一个命令即可看到本机的IP地址。

► 用图解+标注方式讲解知识

本书在介绍内容时，采用单双栏混合排版方式，让内容更加丰富，并采用通俗易懂的语言进行描述，旨在将内容讲清楚，所有内容均配图，通过图文对照+标注的写作方式，读者可以很容易地按照从左到右、从上到下的阅读方式对知识点进行操作学习。



对于单双混排的排版方式，其阅读顺序为：



► 用丰富的栏目插播知识

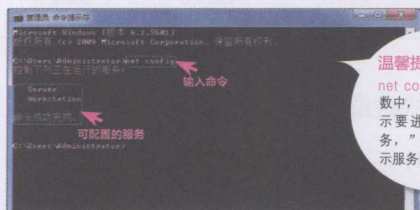
本书在排版时，还使用了丰富的知识插播和温馨提示，让读者获取更多的知识。

知识插播

类似于“聚生网管”的远程控制软件有很多，如“天易成网络管理系统”、“P2P终结者”、“网络执法官”等，其功能都大同小异，有一定软件运用或操作的人使用都比较简单，一般在下载这类软件时也有功能和操作的说明，这里就不再介绍了。



- net config命令：用于显示或更改某项服务的设置。其命令格式为：net config [service] [options]，下图为不带参数显示可配置服务列表。



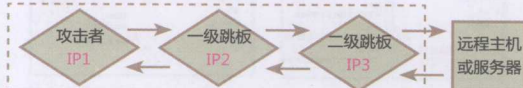
温馨提示：

net config 命令的参数中，“service”表示要进行配置的服务，“options”表示服务的特定选项。

用直观的图示归纳知识

本书对于操作性不是很强的知识点，采用了图示的方式传达给读者，使内容更简练直观、通俗易懂。

- 跳板技术是黑客常用的入侵隐藏技术，其结构如下所示。



入侵者与远程主机之间的数据包都是通过“一级跳板”、“二级跳板”传输的，与远程主机直接接触的只有“二级跳板”主机，因此，即使入侵行为被远程主机发觉，能够直接查出的也就只有“二级跳板”主机，实现了入侵中的隐藏。

Who——读者对象

本书能够帮助读者学习电脑安全及黑客攻防的相关知识，适用于电脑维护人员、IT从业人员，以及对黑客攻防和安全维护感兴趣的读者自学参考，也可作为大中专院校和各种电脑培训班的学习教材。

编者

2013年5月

目录

CONTENTS

第01章

黑客的概述 1

第一节 黑客的基本认识

- 01 黑客是什么 2
- 02 黑客的攻击手段 3
- 03 黑客的攻击流程 4

第二节 黑客与IP地址

- 01 认识IP地址 5
- 02 在本地连接中查看本机IP地址 6
- 03 用命令查看本机IP地址 8
- 04 查看网站的IP地址 9

第三节 端口

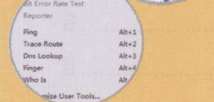
- 01 端口与端口的分类 10
- 02 查看端口 12
- 03 禁用不需要的端口 13

第四节 黑客的常用命令

- 01 ping命令 14
- 02 net命令 16
- 03 ftp命令 23
- 04 netstat命令 25
- 05 tracert命令 29
- 06 其他命令 30



第02章



信息的搜集、嗅探与扫描..... 33

第一节 信息的搜集

- 01 获取IP地址.....34
- 02 查看网站备案信息.....35

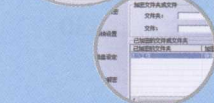
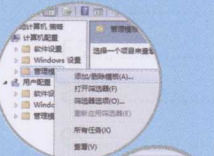
第二节 信息的嗅探

- 01 嗅探器的认识.....36
- 02 使用Sniffer portable捕获数据.....37
- 03 简单的影音神探嗅探器.....41
- 04 捕获网页的艾菲网页侦探.....43

第三节 信息的扫描

- 01 扫描器与端口扫描的分类.....44
- 02 用LanSee搜索局域网的共享资源.....45
- 03 检测系统漏洞.....47
- 04 用X-Scan进行扫描.....48
- 05 SuperScan的简单使用.....51

第03章



基于系统漏洞的入侵与防范..... 58

第一节 系统的安全隐患

- 01 漏洞产生的原因和隐患.....57
- 02 常见系统漏洞列举.....59

第二节 漏洞攻击的防范

- 01 组策略的安全设置.....61
- 02 注册表安全设置.....68
- 03 密码设置.....72
- 04 个人电脑的安全设置.....75

第三节 常见的密码破解

- 01 清除BIOS密码 76
- 02 破解Windows登录密码 78
- 03 破解其他文件的密码 80
- 04 密码破解的防范 81

远程控制技术 82

第一节 基于认证的入侵

- 01 IPC\$入侵 83
- 02 Telnet入侵 87
- 03 连接网络注册表 93

第二节 远程控制的使用

- 01 远程控制任我行 96
- 02 远程控制介绍 104
- 03 远程控制的安全防范 107

基于木马的入侵与防范 111

第一节 木马的基本认识

- 01 木马的特征 112
- 02 木马的结构 113
- 03 木马的种类 114

第二节 木马的攻击原理

- 01 木马的运行 115
- 02 木马的攻击手段 117
- 03 木马的伪装 118





- 04 木马的隐藏..... 120
- 05 木马信息的反馈机制..... 121

第三节 木马工具介绍

- 01 应用程序捆绑器的使用..... 122
- 02 “冰河”木马介绍..... 126

第四节 木马清除与防范

- 01 木马的症状及清除原理..... 131
- 02 用360安全卫士扫描并清除木马..... 133
- 03 手动清除木马..... 137
- 04 预防木马入侵..... 139

第06章

平时上网的黑客攻击与防范..... 140

第一节 QQ攻防

- 01 黑客为什么要攻击QQ..... 141
- 02 黑客攻击QQ的方式..... 142
- 03 QQ消息炸弹..... 143
- 04 QQ聊天记录查询..... 145
- 05 设置QQ密保问题..... 148
- 06 其他QQ密码设置..... 150
- 07 系统安全设置..... 153
- 08 设置QQ空间权限..... 156
- 09 设置QQ点保护..... 158

第二节 电子邮件攻防

- 01 利用电子邮件的攻击..... 160
- 02 网易邮箱的反垃圾设置..... 161
- 03 提高网易邮箱的账户安全..... 162





04 关闭Outlook的预览功能	164
05 为QQ邮箱设置独立密码	165
06 使用邮箱的注意事项	166

第三节 浏览器攻防

01 浏览器攻击的方式	168
02 网页炸弹	169
03 网页炸弹的防范	171
04 为注册表解锁	172
05 使用注册表恢复主页	173
06 删除上网后的历史记录	175
07 IE的安全设置	176
08 预防来自浏览器的攻击	178

第 07 章

安全防范黑客入侵 179

第一节 设置IP和端口

01 为IE设置代理服务器	180
02 用代理服务器登录QQ	181
03 禁用NetBIOS	182
04 创建IP安全策略	183

第二节 网络防火墙

01 认识网络防火墙	190
02 瑞星个人防火墙	192
03 设置Windows防火墙	200

第三节 系统安全处理

01 严格控制运行权限	204
02 控制程序自动下载	205



03 备份注册表.....	206
04 禁止用浏览器查看本地磁盘.....	208
05 禁止修改账户密码.....	209
06 清除卸载程序过程中的残留项.....	212
07 删除多余的右键菜单.....	213

第四节 软件保护系统

01 超级兔子的使用.....	215
02 360安全卫士的使用.....	218

信息隐藏与后门清理.....221

第一节 入侵隐藏技术

01 文件隐藏技术.....	222
02 跳板技术.....	224
03 其他入侵隐藏技术.....	226

第二节 后门账户

01 用“命令提示符”创建后门账户.....	227
02 用注册表创建后门账户.....	229
03 清除隐藏的后门账户.....	232

第三节 常见的其他后门

01 系统服务后门.....	234
02 木马程序后门.....	236

第四节 清除事件日志

01 事件查看器.....	237
02 清除本地电脑的系统日志.....	238
03 其他清除事件日志的方式.....	240
04 禁止用户访问事件日志.....	241

第08章





第一章

黑客的概述

在网络中有一群被称为“黑客”的神秘人物，有时他们义务维护着网络的安全，有时却又以网络破坏者和网络大盗的面目出现。那么，黑客究竟是什么？他们又是怎样操控网络的呢？本章将讲述有关黑客的基本知识，揭秘黑客使用的一些常用命令。





第一节

黑客 的基本认识

01 黑客是什么

黑客究竟是什么呢？是天才，是艺术家，是罪犯还是恶作剧者？或许，黑客已成为他们的综合体。

► **黑客的发展史。**为了更清楚地认识黑客，可以从黑客的发展史开始了解。

① 早期的黑客

最早的黑客并不是攻击者，而是创造者。他们为电脑而生，是真正的程序员，在追求卓越的技术的同时推动了互联网的发展，使电脑世界多了一分生气。

② 20世纪80年代的黑客

随着世界工业化的发展，电脑技术逐渐成熟，一些黑客们把精力放在寻找系统的各种漏洞上，并通过暴露网络系统的缺陷与非法改进服务器等行为来表现技术和反对权威。

③ 现在的黑客

黑客技术已经被越来越多的人掌握，更多的目的是利用黑客技术窃取资料、监视和肆意破坏等行为来获得物质和金钱上的利益。

► **黑客。**原指热衷于电脑技术、水平高超的电脑专家，尤其指程序人员；现在的黑客指那些专门利用网络技术搞破坏或恶作剧的家伙，更有甚者是指攻击别人电脑系统来实现自己利益的人群。



温馨提示：

并不是所有黑客都攻击别人的电脑系统，也有黑客用自己的技术保护着我们的网络。人们习惯将攻击电脑系统的黑客称为“骇客”，他们的行为属于犯罪行为。



温馨提示：

黑客与骇客都是一种技术人员的身份，说法上并没有严格的区分，他们共同推进了电脑技术的发展，已逐渐成为一种文化，根深蒂固，我们只有了解他们，才能有效地预防。

第一节

黑客
的基本认识

02 黑客的攻击手段

黑客技术的发展导致网络世界的安全性不断受到挑战，为了能保障安全上网，就要更多地了解他们的攻击手段。

- **黑客的攻击手段。**分为非破坏性攻击和破坏性攻击两类，前者只为扰乱系统运行，而后者却是真正的入侵、破坏和窃取行为。下面是黑客常用的4种攻击手段。

① 信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。

② 后门程序

电脑完成设计之后需要去掉各个模块的后门，但有时由于疏忽或者其他原因，某些（如便于日后访问、测试或维护）后门没有去掉，黑客就会利用它们来攻击系统。

③ 网络监听

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，是最常用的一种攻击手段。

④ 拒绝服务

拒绝服务又叫分布式DOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统可用资源，最后致使网络服务瘫痪的一种攻击手段。

知识插播

一般黑客的攻击目的有如下所示的几种。

- | | |
|---------------|------------|
| ① 获取超级用户的权限 | ⑤ 对系统的非法访问 |
| ② 获取文件和传输中的数据 | ⑥ 涂改信息 |
| ③ 执行黑客的某种进程 | ⑦ 暴露信息 |
| ④ 进行不许可的操作 | ⑧ 拒绝服务 |



第一节

黑客的基本认识

03 黑客的攻击流程

黑客攻击网络的手段十分丰富，或许在上网的过程中不经意就中了黑客的攻击，令人防不胜防。但是，如果明确黑客的攻击流程，就可以预防黑客的入侵。

- **黑客攻击流程。**黑客进行攻击时都有一个习惯性的流程，其攻击流程大致可分为如下4个阶段。

① 确定目标的IP地址

在攻击之前，要先确定攻击的目标，也就是对方电脑的IP地址。

② 扫描开放端口

了解对方开放了哪些端口，找到进入对方电脑的入口。

③ 破解账号和密码

用黑客手段或工具破解对方账号和密码，入侵对方电脑。

④ 实现目的

在目标主机上进行攻击，从而实现黑客的入侵目的。

知识插播

黑客攻击的具体流程图

