Mc Graw Hill Education

安全技术经典译丛

EXTREME EXPLOITS

Advanced Defenses Against Hardcore Hacks

终极守护

——针对黑客的高级防御技术

Victor Oppleman
(美) Oliver Friedrichs 著
Brett Watson
袁野 关翔 译

清华大学出版社

终极守护

——针对黑客的高级防御技术

Victor Oppleman
(美) Oliver Friedrichs 著
Brett Watson
袁野 关翔 译

清华大学出版社
北京

Victor Oppleman, Oliver Friedrichs, Brett Watson
Extreme Exploits: Advanced Defenses Against Hardcore Hacks
EISBN: 0-07-225955-8

北京市版权局著作权合同登记号 图字：01-2006-4713

图书在版编目(CIP)数据

终极守护——针对黑客的高级防御技术/(美)奥普里曼(Oppleman, V.)，(美)弗里德里奇(Friedrichs, O.)，(美)沃森(Watson, B.)著；袁野，关翔译. —北京：清华大学出版社，2007.7

书名原文：Extreme Exploits: Advanced Defenses Against Hardcore Hacks
ISBN 978-7-302-15481-5

Ⅰ. 终… Ⅱ. ①奥…②弗…③沃…④袁…⑤关… 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(2007)第 090291 号

责任编辑：王 军 刘作舟
装帧设计：孔祥丰
责任校对：胡雁翎
责任印制：孟凡玉
出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175 **邮购热线**：010-62786544
投稿咨询：010-62772015 **客户服务**：010-62776969
印 刷 者：三河市春园印刷有限公司
装 订 者：三河市溧源装订厂
经 销：全国新华书店
开 本：185×260 **印 张**：23.5 **字 数**：572 千字
版 次：2007 年 7 月第 1 版 **印 次**：2007 年 7 月第1 次印刷
印 数：1～4000
定 价：48.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103 产品编号：021834-01

译 者 序

在 Web 技术飞速演变、电子商务蓬勃发展的今天，在线安全风险已达到了前所未有的危险程度。企业在信息安全方面进行了周密的防护，同时对重点网站如电子商务网站等都做了专业的安全加固，但黑客入侵企业的现象仍旧不断发生；企业机密信息泄露呈日益上升趋势；攻击重心已经从主机系统、网络系统转移到应用层面(如网站)，因而企业的 CIO、CSO、网络管理人员及安全管理人员需要不断更新其防范技能。

读者在阅读本书前言的这段时间里，可能至少会公布十几个软件漏洞，另外还可能发现了 20 多个病毒和病毒变体，甚至在 Internet 上至少有四百万个已经被感染的计算机正在试图攻击其他计算机。这些数字仅仅是根据我们掌握的经验数据得出的保守平均值，它们在不断地警示着我们。究竟有哪些正在发生的情况是我们所不知道的呢?

业务和客户所面临的网络攻击增长趋势在近期是不可能有所缓解的，事实上反而会更加恶劣。面对这类规模和复杂程度都在不断增长的攻击，我们中的许多人不得不付出更多的努力来降低风险。

使问题更加复杂化的是：我们平时使用的很多设备都开始通过 IP 地址与网络建立起连接。这不再仅仅关系到我们的服务器、路由器、桌面电脑，还将扩展到我们的电话、PDA、视频游戏操纵台等。令人欣慰的是，安全软件能够帮助我们防御正在扩张的网络，但它们并不是我们所期望的万能钥匙。能够避免发生这些后果的关键是专家掌握的安全知识，他们的目标就是保护我们不受网络攻击增长趋势的影响。

本书作者具有的独到的专业经验是其他参考书中不常见到的。他们不仅负责保护 Internet 主干网络，还致力于安全软件产品开发的前沿，十多年来一直帮助保证“世界 500 强”的公司和世界行政机构的安全。读者在了解幕后核心问题的过程中将形成威胁的概念，并深刻理解涉及防御和进攻两方面的策略和技术，从而能更好地处理我们所面对的充斥着各种安全威胁的网络环境。

在本书的翻译过程中，我们尽量保持了原著的特色。但是为了符合中文语法以及表达的习惯，在能够正确表达英文原意的前提下适当进行了意译，以保证科技图书的严肃性和简洁性。新出现的术语或没有统一译法的术语，我们直接采用英文，或者用英文注释。本书前 10 章由袁野翻译，后 8 章由关翔翻译。如果本书能够对读者有所帮助，那将是我们最大的心愿。

由于译者水平有限，难免存在错误和疏忽，敬请读者多多批评指正，反馈信息请发至 wkservice@tup.tsinghua.edu.cn。

译 者

2006 年 10 月

前　言

欢迎阅读《终极守护——针对黑客的高级防御技术》一书。本书的目的是帮助读者更好地理解和处理新兴的信息安全威胁，并希望将一些经过实践证明的概念和技术与读者一起分享。这些概念和技术是作者在加强保护世界上最易受到攻击的网络和信息资源时总结出来的。本书与以往这方面的参考书相比，在网络和信息安全方面提出了不同的观点。目前市场上关于信息安全的大部分参考书都是通过向读者列出成百上千个脚本或可下载的实例来揭示黑客和反黑客技术的；还有一些则是具体介绍一两个软件包和特定的环境或情形。但是多数情况下，随着工具和策略的不断进化，这些知识很快就过时了。而本书的目标是使读者在了解幕后核心问题的过程中形成威胁的概念，并能深刻理解涉及防御和进攻两方面的策略和技术。有了这些知识作为武装，读者不仅能更好地利用现在的各种工具，还能进而设计出新工具、新技术和面向未来的有效策略。

写给读者的话

本书适合安全专业人员，以及各种相关技术水平的系统和网络管理员。如果你刚成为一名信息安全分析员，那么将满意地发现本书的侧重点不是如何确定和配置工具，而是介绍应该如何使用工具以及它们是如何工作的。你不会在本书中看到一连串的手册指南或网络内容反馈。书中不仅提供了大量使用开源软件的例子，还讨论了适用于商业软件解决方案的概念。可以说，本书对大型和小型机构都十分有用。

如果你是一名技术经理，你将满意地发现作者对工艺和技术的精确解释有助于掌握软件和设备生产商所使用的专业术语，并能为你的员工制作容易理解的威胁和对策的对照表。同样，书中讨论的防御概念将使你成为一个精明的买家，制定出合适的信息安全解决方案。特别要注意每章最后的“防御方案小结”部分，它简单总结了应该采取的最重要的策略措施，以帮助维护网络安全。希望技术经理们能询问自己的员工对每一个工作项目的完成情况，由此来提高他们的防御意识，并共享可能严重影响机构安全的信息。

本书层次结构与关键内容

本书的章节层次结构包括从机构的网络边界一直到对员工 PC 的数字取证分析等方面的内容。第 I 部分是“安全专家眼中的核心 Internet 基础设施”，解释了经常被忽略的 Internet 路由和 DNS(域名服务)中蕴藏的危险；帮助大家理解 Internet 服务提供商如何管理他们的网络，以及机构在没有控制其路由和 DNS 的情况下如何建立网络安全措施。第 II 部分是“网络边界和关键 Internet 基础设施的保护”，这部分涉及到很多热点问题，包括数据包过滤、入侵检测与防御、安全网络结构设计以及 E-mail 等常用应用服务的防御；另外还概要介绍了无线网络的安全防御，包括利用与供应商无关的模板设计安全可靠的无线 LAN，并引入

了一些网络异常检测的新方法。第III部分是“网络漏洞评估”，非常全面地概述了漏洞评估过程。大量的考虑因素和几年的高风险网络审计经验形成了这种已经验证的方法学。最后，第IV部分“应付未来威胁的对策”探究了数字取证、木马和软件开发细节；解释了常见的软件漏洞词源，如“缓冲区溢出(buffer overflow)”和“竞态条件(race condition)”；并介绍了如何避免这些以及其他破坏性软件的问题。

本书每一章都以一个简短的引言和一组关键概念开始，以方便读者了解随后的内容。像大多数技术类图书一样，本书可能不那么引人入胜，所以这些简短的引言能帮读者决定哪些章节现在阅读，哪些章节以后阅读。另一个关键要素是每章最后的“防御方案小结”部分，这章讨论的主要部件所能采取的最重要措施，都简要总结在该部分的列表中。

真诚地希望本书对你能有所帮助，也欢迎你提出宝贵的建议。请访问本书的合作网站(www.extremeexploits.com)获得较新的信息，或者与作者联系。

关于本书合作网站

作者开发的合作网站(www.extremeexploits.com)中提供了一组链接，读者可以从中找到优秀的软件工具以及其他一些有用资料。设计该网站的目的是为了让读者学到本书中所不能囊括的更广泛更精确的知识，并提供一些基于 Web 的工具，以帮助读者进行漏洞评估和其他研究。请访问该网站以扩展本书范围之外的研究。

读者意见反馈卡

亲爱的读者：

感谢您购买了本书，希望它能为您的工作和学习带来帮助。为了今后能为您提供更优秀的图书，请您抽出宝贵的时间填写这份调查表，然后剪下寄到：北京清华大学出版社第五事业部(邮编 100084)；您也可以把意见反馈到 cwkbook@tup.tsinghua.edu.cn。邮购咨询电话：010-62786544，客服电话：010-62776969。我们将充分考虑您的意见和建议，并尽可能地给您满意的答复。谢谢！

本 书 名：_____

个人资料：_____

姓　　名：_____ **性　别：**□男 □女 **出生年月(或年龄)：**_____

文化程度：_____ **职　业：**_____ **通讯地址：**_____

电话(或手机)：_____ **传　真：**_____ **电子信箱(E-mail)：**_____

您是如何得知本书的：_____

□别人推荐 □出版社图书目录 □网上信息 □书店

□杂志、报纸等的介绍(请指明)_____ □其他(请指明)_____

您从何处购得本书：□书店 □电脑商店 □软件销售处 □邮购 □商场 □其他

影响您购买本书的因素(可复选)：

□封面封底 □装帧设计 □价格 □内容提要、前言或目录 □书评广告

□出版社名声 □作者名声 □责任编辑

□其他：_____

您对本书封面设计的满意度：□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书印刷质量的满意度：□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书的总体满意度：

从文字角度：□很满意 □比较满意 □一般 □较不满意 □不满意

从技术角度：□很满意 □比较满意 □一般 □较不满意 □不满意

本书最令您满意的是：

□讲解浅显易懂 □内容充实详尽 □示例丰富到位 □指导明确合理 □其他：_____

您希望本书在哪些方面进行改进？_____

您希望增加什么系列或软件的图书：_____

您最希望学习的其他软件：1._____ 2._____ 3._____ 4._____

您对使用中文版软件或外文版软件介意吗？更喜欢使用哪一种版本？

□介意 □无所谓 □中文版 □外文版

您对图书所用软件版本是否很介意？是否要求用最新版本？

□是，要求是最新版本 □无所谓 □不，因为硬件或软件跟不上要求

您是如何学习最新软件的？

□看计算机书 □看多媒体教学光盘 □自己摸索或查看软件的帮助信息 □参加培训班 □向其他人请教

□其他：_____

您的其他要求：_____

目　录

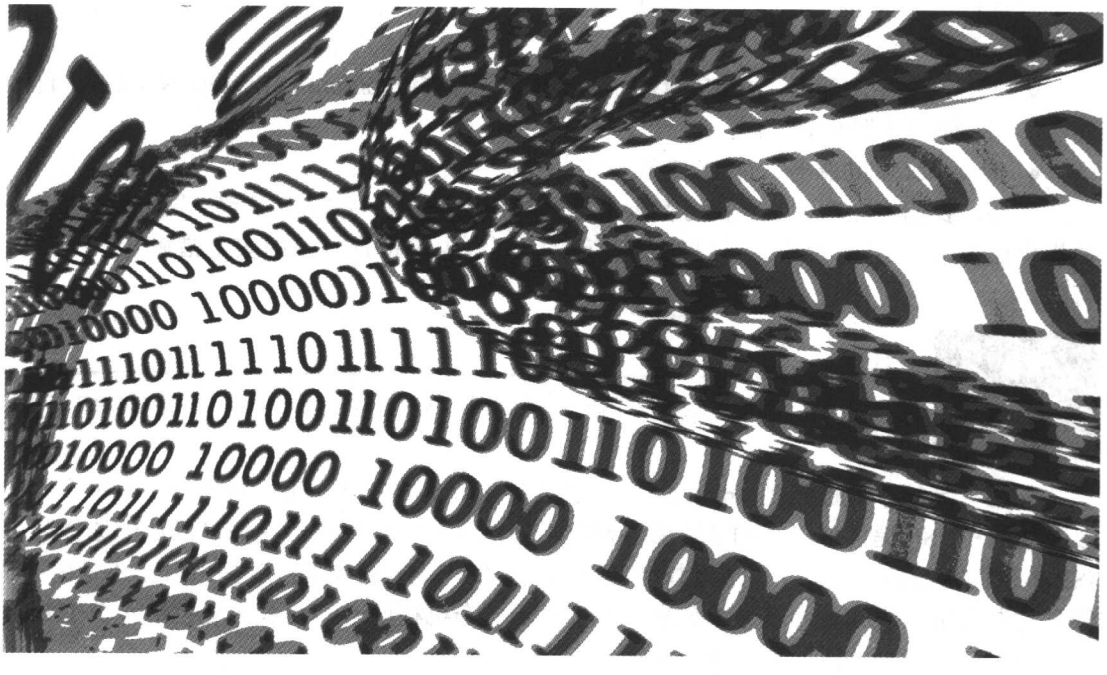
PART

安全专家眼中的核心 Internet 基础设施

CHAPTER

1

安全的 Internet 基础设施



“欢迎来到 Internet——这个世界上最大的 beta 测试版网络。”　　——匿名者

虽然 Internet 已成为当今许多业务的核心技术，但从很多方面来看，它仍然是实验性的网络。随着 Internet 技术的日新月异，新的安全威胁与对抗手段使得 Internet 的体系结构和操作方式不断发生变化。因此，一旦在 Internet 上建立了业务，就应该了解一些有关如何在 Internet 上确保业务安全的知识。

20 世纪 90 年代初，Internet 的发展开始突飞猛进。此时 ISP(Internet service provider，Internet 服务提供商)所提供的服务非常有限，通常只包括物理连接(一般为 fractional-T1、T1 或 DS3)、IP 路由、IP 地址的注册/授权和 DNS 服务。ISP 主要确保机构能够安全地使用边界路由器、物理链路、DNS 以及网络基础设施的核心部分，而与 Internet 连接相关的所有其他方面的安全都由机构负责保证。

如今，ISP 提供的服务范围大大扩展，而且这些服务已经成为了标准 Internet 产品供应的组成部分。如果机构完全依靠 ISP 提供服务，则由 ISP 负责保证安全；如果机构选择自己管理这些服务，则由机构负责保证安全。不管怎样，我们都需要知道这些服务的功能和其存在的隐患，以及黑客是如何利用它们进行攻击的，了解这些能够使我们在选择 ISP 或实现安全时采取正确的措施。

本章将会介绍 Internet 的几个基本功能，实现这些功能的可能是 ISP 或机构自己，也可能是两方共同合作：

- **Internet 基本服务**　如 IP 地址注册/授权、ASN(Autonomous System Number，自治系统号)注册和 IP 路由。
- **Internet 辅助服务**　如 DNS 和电子邮件。

另外，我们将在本章末尾部分简要概括一份问题清单。根据其中所列的问题，可以评估提供服务的 ISP 是否具有可靠的安全策略，同时也可审查自己的安全措施和策略是否有效。

注意

本章中“机构”这个术语一般是指非 ISP 实体，如公司、非盈利性组织等。

如果只是简单地连接到 Internet 上，必然存在大量的安全隐患。事实上，有很多 ISP 以及由这些 ISP 提供或管理的各种服务都能够消除这些安全隐患，我们可以从中选择某个 ISP 提供的部分或全部服务。通过权衡经济和安全的得失，机构可以选择由自己还是由 ISP 管理这些服务。表 1-1 和表 1-2 分别描述了对于一个机构而言，将服务交付给一个 ISP 管理或者由自己管理的风险和好处；可将两者进行比较。

表 1-1　ISP 管理 Internet 服务的风险和好处

ISP 管理的风险	ISP 管理的好处
ISP 承担保证机构网络安全性和可靠性的主要责任，其自身基本上不能对策略和管理进行控制	需要的技术员工较少
当服务中存在问题时，必须与 ISP 进行交互，因此解决问题的时间可能较长	ISP 提供 24 小时网络管理，因此机构不需要自己的员工加班维护网络
一般由 ISP 提供网络设备来管理服务	机构的资金开销较少

表 1-2　机构管理 Internet 服务的风险和好处

机构管理的风险	机构管理的好处
需要更多的技术员工	独立实现安全过程和策略，因此可以控制并保证网络的安全性和可靠性
可能需要技术员工 24 小时轮班值守	比起 ISP，解决问题的速度更快
增加了对网络设备的资金开销	能够自主选择设备供应商

1.1　Internet 基本服务

这一节将讨论大多数 ISP 都会提供的基本服务，这些服务已经成为了通用 Internet 连接的组成部分。我们将介绍分配和注册 IP 地址或者 ASN(自治系统号)时常会出现的错误，并讨论有关 Internet 路由以及边界路由器的一些鲜为人知的安全问题。

1.1.1　IP 地址(前缀)的分配和注册

一个机构除了要获得与ISP的物理连接外(参阅第4章)，还必须获得IP地址块(IP前缀)。这个IP地址块由ARIN(北美Internet号码注册管理机构)直接分配(中国则由CNNIC或APNIC分配，译者注)，或者由 ISP 再分配。不管哪种情况，以正确的方式注册 IP 前缀是保证数据不被黑客篡改的关键。

注意

北美洲和南非的机构从 ARIN 获得 IP 地址，LACNIC(拉丁美洲及加勒比地区网络信息中心)为南美洲的机构提供服务，APNIC(亚太网络信息中心)负责亚洲机构的服务，RIPE NCC(欧洲网络协调中心)为欧洲和北非的机构提供服务。

无论是 ISP 还是 ARIN，申请机构都需要提交其对 IP 前缀大小的请求。对于机构的 IP 地址请求，不同的 ISP 有不同的处理程序。而 ARIN 制定的处理规则及程序相比 ISP 要更加严格，在其官方网站的首页(http://www.arin.net/registration/index.html)点击“Registration”

链接，可以看到相关文档。

当 ISP 或机构向注册管理机构提交有关 IP 前缀的注册信息时，需要利用应用角色账户(role account)来表示所有网络联系点(point of contact，POC)记录和联系账户编码(contack handle)——在 RFC 2142 文档中有针对它们的规定。角色账户是 E-mail 的别名，在机构的邮件系统中，监控邮箱/分配列表的技术人员习惯把 E-mail 称为角色账户。因为 RFC 不会特别处理 ARIN 中的注册数据，所以我们在这里也使用“角色账户”这个概念。下面描述的是正确注册了 IP 前缀后，在 ARIN 数据库中显示的数据结果。

```
OrgName:     Internet Assigned Numbers Authority
OrgID:       IANA
Address:     4676 Admiralty Way, Suite 330
City:        Marina del Rey
StateProv:   CA
PostalCode:  90292-6695
Country:     US

NetRange:    192.0.2.0 - 192.0.2.255
CIDR:        192.0.2.0/24
NetName:     IANA
NetHandle:   NET-192-0-2-0-1
Parent:      NET-192-0-0-0-1
NetType:     Reassigned
Comment:     Please see RFC 3330 for additional information.
RegDate:
Updated:     2002-10-14

OrgAbuseHandle:  IANA-IP-ARIN
OrgAbuseName:    Internet Corporation for Assigned Names and Number
OrgAbusePhone:   +1-310-301-5820
OrgAbuseEmail:   abuse@iana.org

OrgTechHandle:   IANA-IP-ARIN
OrgTechName:     Internet Corporation for Assigned Names and Number
OrgTechPhone:    +1-310-301-5820
OrgTechEmail:    abuse@iana.org
```

这个例子中，请注意 Technical 和 Abuse 两个联系账户编码，它们显示的是角色账户信息，而不是机构内部的个人信息。注册 IP 前缀最重要的一点就是提供的机构联系信息应该与个人无关。比如，机构内部的一个网络管理员以机构的名义注册了一个 IP 前缀，但联系账户编码却注册为他的个人信息。假设这个管理员后来因为不满离开了这个机构或被辞退了，那么他可能会冒充机构的技术联系人与 ARIN 取得联系，并请求改变如机构名称和联系信息等内容；他甚至会把 IP 前缀返回给 ARIN，使得该地址前缀被分配给另一个机构。这种情况虽然很少出现，但还是有可能发生的。尽管 ARIN 有严格的规则阻止类似情况的发生，但 ISP 和机构还是应使注册的机构信息与个人无关，从而降低数据被未经授权的人恶意篡改的风险。

同时，机构还应该保证公司名称、街道地址和电话号码的正确性和时效性，这样有利