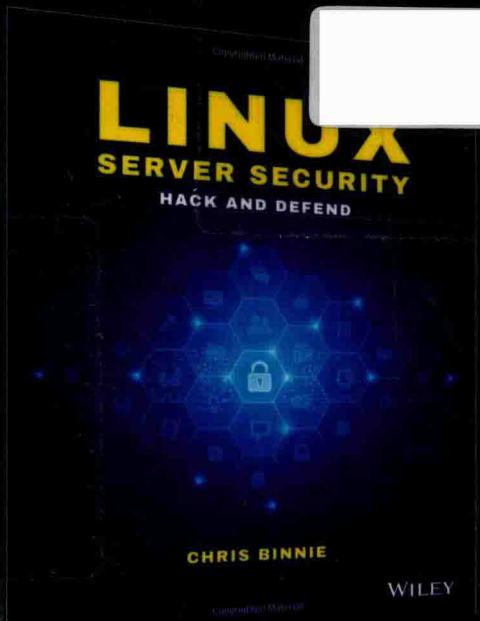
WILEY

安全技术经典译丛

Linux服务器安全攻防

Linux Server Security: Hack and Defend



[美] Chris Binnie 著
田洪 译

清华大学出版社

安全技术经典译丛

Linux 服务器安全攻防

[美] Chris Binnie 著

田洪 译

清华大学出版社

北 京

Chris Binnie
Linux Server Security: Hack and Defend
EISBN：978-1-119-27765-1

图书在版编目(CIP)数据

Linux 服务器安全攻防/(美) 克里斯·宾尼(Chris Binnie) 著；田洪 译. —北京：清华大学出版社，2017
(安全技术经典译丛)
书名原文：Linux Server Security: Hack and Defend
ISBN 978-7-302-45792-3

Ⅰ. ①L… Ⅱ. ①克… ②田… Ⅲ. ①Linux 操作系统—安全技术 Ⅳ. ①TP316.85

中国版本图书馆 CIP 数据核字(2017)第 288060 号

责任编辑：王　军　韩宏志
装帧设计：牛静敏
责任校对：曹　阳
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京泽宇印刷有限公司
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：5.5　　**字　　数**：148 千字
版　　次：2017 年 1 月第 1 版　　**印　　次**：2017 年 1 月第 1 次印刷
印　　数：1～3000
定　　价：39.80 元

产品编号：072275-01

译 者 序

Linux 是一套免费使用和自由传播的类 Unix 操作系统，是一个基于 POSIX 和 Unix 的多用户、多任务、支持多线程和多 CPU 的操作系统。它能运行主要的 Unix 工具软件、应用程序和网络协议。它支持 32 位和 64 位硬件。Linux 继承了 Unix 以网络为核心的设计思想，是一个性能稳定的多用户网络操作系统。

Linux 操作系统诞生于 1991 年 10 月 5 日(这是第一次正式向外公布的时间)。Linux 存在着许多不同的 Linux 版本，但它们都使用了 Linux 内核。Linux 可安装在各种计算机硬件设备中，比如手机、平板电脑、路由器、视频游戏控制台、台式计算机、大型机和超级计算机。

Linux 与其他操作系统一样，也存在安全隐患。而随着它在全世界范围内的普及使用，目前针对它的攻击越来越多，安全事件也呈上升趋势，形势非常严峻。要想在技术日益发展、纷繁复杂的网络环境中，保证 Linux 系统的安全性，需要切实做好事前预防以及事后恢复工作。

本书共分为 10 章，从不同侧面介绍了 Linux 系统安全攻防的相关内容。读者可按任何顺序阅读本书所包含的所有章节，并且这些章节汇聚了多年来作者作为一名 Internet 用户所感兴趣的一些安全主题。

本书图文并茂，技术新，实用性强，以大量的实例对相关内容做了详细解释，是Linux系统管理员不可缺少的实用参考书籍。

参与本书翻译的人有田洪、范园芳、胡训强、纪红、晏峰、余佳隽。最终由田洪负责统稿，在此一并表示感谢。此外，还要

感谢我的家人，她们总是无怨无悔地支持我的一切工作，我为有这样的家庭而感到幸福。

译者在翻译过程中，尽量保持原书的特色，并对书中出现的术语和难词难句进行了仔细推敲和研究。但毕竟有少量技术是译者在自己的研究领域中不曾遇到过的，所以疏漏和争议之处在所难免，望广大读者提出宝贵意见。

最后，希望广大读者能多花些时间细细品味这本凝聚作者和译者大量心血的书籍，为将来的职业生涯奠定良好基础。

译者

作者简介

Chirs Binnie 是一名技术顾问，使用 Linux 系统进行在线工作近二十年。在他的职业生涯中，在云端以及银行和政府部门部署过许多服务器。他曾在 2005 年构建了一个自治系统网络，并通过自己构建的媒体流平台为 77 个国家提供高清视频，同时多年来还为 *Linux Magazine* 以及 *ADMIN Magazine* 撰写技术文章。工作之余，Chirs 喜欢户外运动，观看 Liverpool FC，并连连称赞 Ockham 刮胡刀的优点。

技术编辑简介

Rob Shimonski(www.shimonski.com)是一位有经验的企业家和商业社区的积极参与者。Rob 是一名畅销书作者和编辑，有超过 20 年的经验，以书籍、报刊、杂志等形式开发、生产和分发印刷媒体。如今，Rob 已经成功帮助出版了超过 100 本目前流行的图书。Rob 曾为无数客户提供过服务，包括 Wiley Publishing、Pearson Education、CompTIA、*Entrepreneur magazine*、Microsoft、

McGraw-Hill Education、Cisco 以及 National Security Agency。此外，Rob 还是一位专家级的架构师，在协议捕捉和分析以及 Windows 和 Unix 系统的工程方面拥有丰富的技术经验。

序　言

众所周知，如果想要以一种有效方式保护系统和网络的安全，则需要与时俱进，不断更新自己的知识。然而，并不是所有技术专业人员都想成为一名全面的安全专业人员；相反，他们更愿意专注其他方面，尽管他们所担负的角色要求掌握与安全相关的知识。

似乎每隔一天都会有新闻报道发生了骇人听闻的黑客攻击，从而使相关领域的人员庆幸自己的客户端未成为攻击的目标。随着我们对响应式连接以及精心编写的软件依赖程度的不断提高，成功地保护一个在线服务会得到很好的回报。

撰写本书旨在对系统和网络所面临的威胁进行概述。本书并不会重点介绍在线安全的某一具体方面，而是旨在通过介绍多个不同的领域，使读者具备足够的知识，以便可以更详细地学习自己感兴趣的内容。本书的每一章探讨了我作为一名 Internet 用户所感兴趣的安全方面。

本书之所以介绍多种不同的主题，其目的是希望帮助读者确保自己的在线服务安全，同时提供机会让读者体验一下黑客常用的一些工具。这样做会让每个读者都受益，特别是可以帮助技术专业人员更好地理解黑客如何识别并尝试利用系统或网络的漏洞。可运用本书所介绍的相关知识摧毁在线服务、窃取数据以及显示加密密码，甚至可以完成其他更强大的功能。

前　言

请思考一下，即使是高度公开的网络攻击，实施起来可能也是非常简单的。对一个系统或者网络发动攻击所包括的步骤可能会非常复杂，也可能会出奇简单。这取决于一个系统是否因为使用了一些众所周知的漏洞软件而使其处于不安全的状态。

一名缺乏经验的黑客的常用攻击手段可能只是永无休止地对端口进行自动化扫描，然后打开一个连接并及时关闭，或者不断搜索 Banner 信息，从而弄清楚在端口后面监听的服务的版本号。如果发现的任何版本号与漏洞数据库中所列出的版本号相匹配，那么黑客就确定了一个新的攻击目标。从这一点上讲，由于该攻击方法几乎完全是自动完成的，因此你可能会认为这无非是计算机攻击计算机而已。

相反，经验丰富的黑客会使用各种不同的方法获取或破坏对某一系统或者网络的访问。他们不仅经验丰富且才智过人，狡猾难防，而且富有创新性、耐心。他们通常充分利用社会工程学，构建自己的硬件并完成各种攻击手法。在攻击过程中，黑客们根据防御者的情况调整手法，此外攻击还会不断演变(有时甚至是快速演变)。大多数攻击所产生的影响取决于是否进行了精心准备；在最开始的侦测过程中，有相当数量的攻击途径会被侦测到。

确保在线服务的安全有点类似于缘木求鱼，虽然我很不愿意这么说，但事实是，不管对一个服务或者系统如何进行安全保护，总会有一种方法违反或者破坏这种保护。因此可以大胆地做这样一种声明，请记住，即使一个系统或者网络当前不易遭受攻击，但在未来某一时刻也极可能会遭到攻击。

这也就意味着，除非破坏服务器或者网络设备的电源，否则打开任何电子设备都意味着打开了一条黑客可以利用的攻击途径。事实是，技术专业人员长期面临着这种情况。因此，在确定网络安全所采用的方法时，需要在黑客可在多大程度上利用在线系统和网络的漏洞，以及用来保护系统和网络安全所花费的预算之间进行权衡。此外，还可以尝试降低单个服务器的风险，例如，将电子邮件服务器与 Web 服务器分开。如果一个计算机集群被黑客攻破，那么理想状态下其他集群则不应该受到影响(前提是这些计算机集群在后台使用了不同的防火墙并且都拥有一个替代的操作系统)。

但也不要过于恐慌，值得庆幸的是，目前经验极其丰富的攻击者实际上并不是很多(对于这些黑客高手，任何防御措施或多或少都会失败，有时甚至只需要数分钟时间就可能攻破)。然而，随着 Internet 的逐步发展，熟练的攻击者可以利用其他被攻破的系统和服务的功能进行攻击，从而对那些不知情的受害者产生令其头痛的问题。

此外，攻击者发动攻击的动机也在发生变化，有时甚至是不可预测的。这些动机可能包括从黑客社区获取相关的荣誉，想证明自己比受害者高出一筹，为崇拜自己的新手进行一次训练演习，或者只是想获取经济利益。另外，根据最常见的统计，也不要忘记那些单纯寻求刺激的人。

如果你的服务容易引起某些类型的不必要的注意，比如 Web 应用程序持续被某些用来查找安全漏洞的探头所探测，那么常识告诉我们，你主要关注的是让开发人员修补应用程序的安全漏洞。相反，如果正在提供一个 E-Mail 服务，就需要绝对确保用来在集群中所有邮件服务器之间读取邮件信息的软件保持最新，并进行经常和及时的修补。只要注意到了最明显的漏洞，就可以大大减少可能暴露给中等水平攻击者的攻击面，同时也能减少他们获取一个立足点进而攻击其他系统的概率。一旦确保了主要的攻击途径基本是安全的，就可以集中精力解决那些不怎么明显的

安全漏洞。

以下几个简单问题有助于将注意力集中在系统或者网络安全上。第一个问题是你正在尝试保护什么内容？例如，隐藏在数据库深处的敏感、机密信息，访问这些数据通常需要通过多个防火墙以及堡垒主机(bastion hosts)，或者正在保护一个需要全天候为用户提供服务的在线服务。该问题非常重要，因为它直接影响到加强防御的手段以及防御策略的选择。例如，你可能愿意每月为网络流量清洗服务(network-traffic-cleaning service)支付高昂的费用，从而免受拒绝服务(Denial-of-Service)攻击，而不会愿意购买多个价格昂贵且高端的硬件防火墙来进行保护。

第二个问题是如何遏制一个安全漏洞？如果网络上的一台服务器或者设备被攻破了，那么是否自动意味着其他主机也将遭遇相同的厄运？如果是，则无疑表明你的安全策略存在需要解决的严重问题。

第三个问题是如何从安全漏洞中恢复？你可能关心的是一旦攻击者发现了冗余信息的工作原理会发生什么事情，以及在什么阶段故障转移服务(failover service)会被激活。如果在完全不知道攻击者是如何攻破安全措施的情况下，只是简单地重新构建主服务器或者盲目地恢复服务，那将是非常困难的。此时你是否可以使用替代供应商的设备或者软件快速恢复服务呢？如果可以，则可以大大减少相同的攻击再次攻陷系统的可能性，并且可以在弄清楚攻击者入侵的方式之后恢复一部分(甚至全部)服务。

本书的组织结构

可按任何顺序阅读本书包含的所有章节，并且这些章节汇聚了多年来作者作为一名 Internet 用户所感兴趣的一些安全主题。

这些主题包括过去、现在以及未来攻击的相关理论，对不同在线攻击的防御，以及授权读者自己进行恶意攻击的方法(其目

的是帮助读者学习如何防御此类攻击)。

通过将不同主题分解到不同章节中，便于读者进行参考，同时可以在未来的学习中返回到这些章节，更详细地学习有关内容。各章的内容如下所示：

第 1 章：隐身斗篷。如果攻击者无法看到你的服务器，并且没有意识到它们的存在，就不会有任何的攻击途径会被利用。该章主要讨论和介绍如何在产品中持续使用服务而又不会引起攻击者不怀好意的关注。

第 2 章：对文件应用数字指纹。可使用多种方法来保证服务器文件系统的完整性，从而确保攻击者无法进行访问。在该章，主要介绍一种手动方法以及一个用来检查黑客程序的自动化工具。

第 3 章：21 世纪的 netcat。多年后，netcat 的最新版本已成为众多黑客所选用的工具(这得益于它所提供的众多高级功能)。在该章，将学习如何识别黑客是否使用此工具攻击服务器，以及学习如何利用这些业界领先的功能。

第 4 章：拒绝服务。只有世界上一些最大型的 Internet 基础设施提供商可以经受得起成熟的、高容量的分布式拒绝服务(Distributed Denial of Service，DDoS)攻击所带来的影响。在该章，将详细讨论该主题，并且会就一个国家因为此类攻击而三个星期失去 Internet 连接这一事件展开评论。

第 5 章：Nping。对于黑客攻击来说，知道某一主机正在运行哪些服务只是成功了一半。功能强大的 Nmap 安全工具的扩展功能允许对任何主机进行检查，并生成带有独特有效载荷的自定义数据包。

第 6 章：日志探测。虽然某些针对服务器执行的探测可能并没有太大的危害，但了解这些探测的工作原理无疑会更有利于进一步保护服务器的安全。在该章，将介绍攻击者探测服务器漏洞点所涉及的相关内容。

第 7 章：Nmap 功能强大的 NSE。许多用户都用过 Nmap 来

完成简单的端口扫描，但很少有人知道该安全工具还包括了攻击远程计算机的功能。在该章，仅讨论默认情况下 Nmap 所附带的众多脚本中可以完成的部分攻击行为。

第 8 章：恶意软件检测。多年来一直困扰 Windows 系统的完全无声的威胁主要来自于以非法形式安装的软件。恶意软件给系统带来的危害是多方面的，从经常弹出令人讨厌的弹出式窗口，到成熟的在线银行攻击。在该章，将学习如何在 Linux 系统上配置一个复杂、频繁更新的反恶意软件解决方案。

第 9 章：使用 Hashcat 进行密码破解。技术专业人员曾经被警告说有一款密码破解工具几乎可以保证破解哈希密码。这意味着一旦非法获取了对哈希密码的访问，那么黑客看到密码内容就只是时间问题。该章将一步一步地完成该过程。

第 10 章：SQL 注入攻击。在一次著名的调查中，SQL 注入攻击被列为最流行的在线攻击。虽然该攻击类型的出现可追溯到 20 世纪 90 年代末，但如今还是有大量的此类攻击通过简单的编程实践成功攻破了企业网站以及关键的在线服务。该章首先讲述了一些有用的历史信息，然后逐步指导如何识别和攻击脆弱的在线服务。

本书读者对象

本书主要面向中等水平的管理人员、软件黑客以及其他 IT 专业技术人员。然而，本书的编写方式可以帮助那些好奇的读者根据自己感兴趣的安全问题快速找到适合的对应章节，同时不需要深入了解 Linux 命令行。本书旨在帮助某些读者更深入地研究特定章节的相关主题，从而进一步扩展有关该主题的知识，同时了解一下其他方面的主题，以便日后参考使用。

另一方面，虽然每章都使用了命令行(对于初学者来说还是需要花费一些时间来学习的)，但对于读者的经验水平却没有太

高的要求。

小结

希望通过本书的学习，你可以了解黑客所使用的工具以及思维方式，从而站在最新安全技术发展的制高点，这样就可以避免以下事情的发生：不再控制自己的系统或网络，而是由其他人来控制。

目　录