HZ BOOKS
华章IT

·网络空间安全技术丛书·

BUILDING ENTERPRISE SECURITY WITH OPEN SOURCE SOFTWARE

# 企业安全建设入门

## 基于开源软件打造企业网络安全

刘焱 编著

百度安全专家撰写，零基础、低成本搭建企业安全防御系统
多位业界专家联袂推荐

机械工业出版社
China Machine Press

# 企业安全建设入门

## 基于开源软件打造企业网络安全

BUILDING ENTERPRISE
SECURITY WITH
OPEN SOURCE SOFTWARE

刘焱 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

企业安全建设入门：基于开源软件打造企业网络安全 / 刘焱编著 . —北京：机械工业出版社，2018.2
（网络空间安全技术丛书）

ISBN 978-7-111-59070-5

I. 企… II. 刘… III. 互联网络 - 安全技术 IV. TP393.408

中国版本图书馆 CIP 数据核字（2018）第 025442 号

# 企业安全建设入门：基于开源软件打造企业网络安全

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：吴　怡　　责任校对：李秋荣
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2018 年 3 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：21
书　　号：ISBN 978-7-111-59070-5　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

华章IT
HZBOOKS | Information Technology

# 对本书的赞誉

本书作者在百度从事安全工作多年，具有丰富的实践经验，他在书中详尽分享了这些干货，对于想要了解、从事企业安全设计、运维的人具备很强的指导意义。

——云舒，默安科技 CTO

企业安全建设受限于两个条件：资金投入有限和最佳安全实践匮乏。兜哥从解决企业安全有效性和最佳实践出发，关注企业安全建设最后一公里，将开源和最佳实践相结合，为企业安全负责人提供了宝贵经验。强烈建议企业安全负责人都能阅读这本书，定能让阅读者受益匪浅。

——聂君，安信证券安全总监

如何快速构建企业安全体系是安全管理员的首要任务，作者将自己在互联网企业多年的安全实践经验汇集成册，不仅介绍了许多优秀的开源产品，还包含了作者对技术选型的思考。全面、实用是本书最大的特点，具备很强的实践指导价值。

——董志强，腾讯云鼎实验室负责人

本书特别贴近互联网公司安全体系从零到一的建设需求，涵盖面广且兼顾深度，安全防护体系自研必备手册。

——kkqq，资深安全专家

威胁情报在国内刚刚起步，引起了广大企业和用户的高度关注，很多信息化和安全较为领先的企业已开始了威胁情报方面的应用实践。本书用一个章节简明扼

要地介绍了国内外几个主流的威胁情报分析平台，是很好的威胁情报分析入门学习材料。

——薛峰，微步在线 CEO

安全源于攻防，随着攻防对抗的升级，每十年就要更新一次安全观。本书以现代化企业安全体系建设为视角，以开源软件为切入点，从准入、加固，到威胁情报、态势感知、业务风控，既有原理的描述，又有开源软件的实践指南，是一本“文不甚深、言不甚俗”的企业安全建设实战宝典，实属 CSO 的案头佳品，值得一读。

——张晓兵，途隆云 CEO

本书理论结合实践，深入浅出地讲解了互联网安全常见的安全问题，可以让读者全面了解安全技术前沿，本书是一线安全工程师必备的随身宝典。

——窦喆，运维帮创始人

本书从互联网企业所涉及的数据、网络等安全风险出发，详细介绍了如何使用开源软件为企业实施安全解决方案，是一本少有的企业安全经典之作。

——赵广，运维派社区发起人，天天学农合伙人

# 序

纵观人类发展的历史，已经先后经历了农业革命、工业革命、信息革命。每一次产业技术革命，都给人类社会带来巨大而深刻的影响。伴随着云计算、物联网、大数据、移动互联网、人工智能等技术引领的数字化变革，全球各个市场、各个行业已经紧密地联系为一个统一体。

数据显示，2015 年中国信息经济规模已经超过 18 万亿元，电子商务交易额超过 20 万亿元，数据总量已经超过 1000 亿元，占全球数据总量的 13%。可以预见，未来 5 年中国大数据产业规模年均增长率将超过 50%，到 2020 年中国的数据总量将超 8000 亿元，占全球数据总量的 20%，届时中国将成为世界第一数据资源大国和“全球数据中心”。每个硬币都有两面，信息经济是推动经济发展的新动能，潜力巨大，前景广阔，与此同时，各类麻烦与威胁也接踵而至。

2016 年 10 月，美国从东海岸的波士顿、纽约、华盛顿，到西海岸的洛杉矶、旧金山和西雅图互联网服务全面宕机。包括 Twitter、Paypal、Spotify 在内多个人们每天都用的热门网站被迫中断服务。据了解，此次“断网”事件是由于美国最主要 DNS 服务商 Dyn 遭遇了大规模 DDoS 攻击所致。攻击者使用了一种叫作“物联网破坏者”的 Mirai 病毒来进行肉鸡搜索。其中，这些设备中有大量的 DVR（数字录像机，一般用来记录监控录像，用户可联网查看）和网络摄像头（通过 Wifi 来联网，用户可以使用 App 进行实时查看的摄像头）。媒体将此次事件形容为“史上最严重 DDoS 攻击”，不仅规模惊人，而且对人们生活产生了严重影响。2017 年 5 月 12 日起，全球范围内爆发基于 Windows 网络共享协议进行攻击传播的蠕虫恶意代码，这是不法分子通过改造之前泄露的 NSA 黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。五个小时内，包括英国、俄罗斯、整个欧洲以及中国的多个高校校

内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件，对重要数据造成严重破坏。各类安全事件已经成为日常新闻的头版常客，严重影响着各种社会经济活动。值得关注的是，分析师们开始把网络攻击事件和严重级别的飓风相提并论，全球网络攻击事件造成的经济损失可能高达 500 多亿美元。

这是最好的时代，也是最坏的时代。《中华人民共和国网络安全法》已于 2017 年 6 月 1 日起施行。这是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。《中华人民共和国网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。这对企业安全运营者提出了严格的要求。

兜哥在书中所阐述的企业安全建设内容，涉及网络安全的方方面面，包括从办公网到业务网的防护系统建设与基础加固，涵盖网络从外到内的全过程，涉及网络准入技术、蜜罐与攻击欺骗技术、数据库安全技术、SIEM/SOC 系统技术、数据防泄密技术和 SDL 与代码审计技术，以及威胁情报的落地、风控系统建设，到整个企业的安全态势感知系统建设。书中特别提到了对 Web 业务系统的防护与加固建议。由于多年来网络技术的发展，特别是 Web 2.0 技术的大范围普及，攻击者们早已将注意力从以往对网络服务器的攻击逐步转移到了对 Web 应用的攻击上。根据 Gartner 调查显示，信息安全攻击有 75% 都是发生在 Web 应用而非网络层面上。同时，数据也显示，三分之二的 Web 站点都相当脆弱，易受攻击。作为国内第一个推出 Web 2.0 漏洞扫描产品的公司，安赛科技通过多年来对国内用户的深入接触发现，目前绝大多数企业还是将大量的投资花费在网络和服务器的安全上，并没有从真正意义上检测 Web 应用本身的安全，这也就给了攻击者以可乘之机。因此，安赛科技于 2013 年在行业内率先推出了基于全流量的大数据分析产品——漏洞感知，利用双向数据流检测技术与 Web 完整攻击周期架构，可以实现对攻击的预判与精准报警，该产品广受好评。2016 年 12 月 27 日，国务院全文刊发了《“十三五”国家信息化规划》，再

次强调了态势感知的重要性。“十大任务”中的最后一项是健全网络安全保障体系，提出“全天候全方位感知网络安全态势”。对这些技术，兜哥在书中做了详尽的阐述，据我提炼理解，主要包括资产识别、漏洞扫描、攻击监测，以及安全的可视化几个方面。

本书是兜哥多年从业经验的真实写照，可谓是呕心之作。在万物互联时代，已经没有可以独善其身的安全孤岛，只有相对安全和不安全的各种子生态。企业安全建设者、运营者在日常工作过程中，需要整体把控，综合考量，可以接受某种程度上的渗透和泄露，只需要把风险控制于可接受范围之内，避免出现破窗效应，否则任何安全措施的效果都会大打折扣，进入“死环”。

近些年，随着安全行业蒸蒸日上，越来越多的公司认识到安全的重要性，逐步建立自己的安全团队。但工作十年、经验丰富、适合负责整个安全团队的人在业内非常稀少，且很多公司在一开始也没有魄力投入巨大成本在一个安全人才上，因此很多公司的安全需求变成了机会，流动到了年轻一辈的安全工程师手里。我相信，阅读本书也是一个机会，本书为广大的安全工程师提供了一个重要的抓手。

林榆坚，安赛科技 CEO

# 前　言

十年前，因机缘巧合，我进入了安全这个行业，而且在一个公司干到现在。当时公司虽然已经很有名气，但是体量和现在比起来还是很小，安全防护体系还非常脆弱。我的第一个项目就是开发公司的准入系统，当时公司其实已经从国外购买了商业准入系统，而且号称是当时 Gartner 全球排名前几名的产品，但是在公司具体环境下这个系统却没有办法很好地运行，无论是易用性、可管理性甚至是基础的安全性，都出过问题。老外的售后支持也就那样，对出现的几次事故也没给出让人信服的解释。最后我们老大，也就是传说中“我的华为十年”那篇文章的作者家俊，决定自己开发准入系统。我们两个小伙伴初生牛犊不怕虎，硬是用三个月开发出了第一版，后面我们按照部门、楼层、总部大厦、分公司的顺序在全集团范围推广，这个系统已经服役到现在。也就是从这个项目起，我对开源软件产生了浓厚的兴趣，并尝试在后面的企业安全建设中使用，从 SNORT、OSSIM、Kippo 到 OSSEC、OpenSOC、Kong 等，我都调研或者使用过。坦诚讲，开源软件存在可管理性差、运营压力大等问题，尤其在专业性要求特别强的领域，比如 APT、防火墙和硬件令牌领域，使用商业安全产品比自己研发工具性价比更高。但是开源软件容易上手、可高度定制、可扩展性强，事实上整个互联网就是基于开源软件发展起来的，使用开源软件在互联网公司做安全也是一个不错的选择。我最近三年主要负责公司对外的商业安全产品，我发现很多模块可以直接使用开源软件，比如 Storm、Kafka、ELK、Celery、Hadoop、TensorFlow 等，这些开源软件都可以让我们不重复造轮子，把精力放在更核心的安全检测能力和业务逻辑上。

本书的第 1 章概述开源软件和网络安全的关系。第 2 章开始介绍互联网公司的防护体系建设，涉及 WAF、抗 DDoS 攻击和服务器主机安全。第 3 章介绍业务网的基础安全加固，包括资产管理、补丁管理、操作系统加固等内容。第 4 章介绍这

几年非常火的威胁情报，并且从开发角度介绍了其中常见的几种威胁情报源的获取方式。第 5 章介绍业务风控，并详细介绍了如何使用 Kong 保护 API 接口。第 6 章介绍代码审计，并详细介绍了如何使用 RIPS 做 PHP 代码审计。第 7 章介绍蜜罐的相关知识，并详细介绍了几种常见的开源蜜罐的使用方法，包括 Glastopf、Kippo、Elasticpot 和 Beeswarm。第 8 章介绍态势感知系统，并分别介绍了如何使用开源软件做漏洞扫描、入侵检测。第 9 章介绍如何使用开源软件建设 SOC 系统，整个架构都是基于 OpenSOC 的。第 10 章介绍数据库安全，并详细介绍了如何使用 DBProxy 充当数据库防火墙，使用 mysql-audit 进行主机端数据库审计，使用 MySQL Sniffer 进行数据库流量审计。第 11 章介绍办公网如何防止数据泄露。第 12 章介绍如何进行办公网加固和基于开源软件开发准入系统。

本书的每个章节都会介绍国内外对应的一些商业安全产品，国外厂商列表主要来自业内比较认可的 Gartner 发布的数据，国内数据主要来自“安全牛”的安全全景图，大家可以根据实际情况选择使用商用产品还是基于开源软件 DIY。本书并不是介绍商业产品的黄页，而且安全创业公司近几年如雨后春笋般成长，所以有遗漏之处敬请原谅。

我一直有个想法就是用我写书的钱开一个烧烤店，虽然目前看开个烧烤摊也勉强，但是我会继续努力，所以本书的演示环境都是基于我假想的在线烧烤网站 www.douwaf.com，该网站基于 Nginx +PHP+ MySQL 架构，部署了 phpMyAdmin 和 WordPress，整个环境在我购买的云主机上。

在这里我要感谢我的家人对我的支持，本来工作就很忙，没有太多时间处理家务，写书以后更是花费了我大量的休息时间，我的妻子无条件承担起了全部家务，尤其是照料孩子方面的繁杂事务。我很感谢我的女儿，写书这段时间几乎没有时间陪她玩，她也很懂事的自己玩，我也想用这本书作为她的生日礼物。我还要感谢编辑吴怡对我的支持和鼓励，让我可以坚持把这本书写完。最后还要感谢各位业内好友在编写本书时对我的各种形式上的支持，排名不分先后：聂君 @ 安信证券、Killer@ 腾讯、刘长波 @ 云堤、云舒 @ 默安科技、薛峰 @ 微步在线、大路 @ 天际友盟、林榆坚 @ 安赛、廖威 @ 易宝支付、sbilly@360、帮主 @ 运维帮、赵广 @ 运

维派、张婉桥 @360。最后我还要感谢我的亲密战友哲超、新宇、子奇、月升、张琳、碳基体、刘超、王胄、吴梅，以及曾经一起的战友徐家俊、黄颖、冯永校、林健、刘秀英、王龙、阮小伟、程伟、彭正茂、刘永树、李亚强、吴登辉、张雨霏、高磊、邵杨民、王致桥、赵铁壮、张浩、刘铁铮、张东辉、李婷婷、程岩、宋柏林、王志刚、吴圣、刘袁君、王珉然，咸鱼。

本书面向运维和安全行业从业者，以及信息安全爱好者、开源技术爱好者。我平时在 Freebuf 专栏以及“i 春秋”分享企业安全建设以及人工智能相关经验与最新话题，同时也运营我的微信公众号“兜哥带你学安全”，欢迎大家关注并在线交流。本书使用的代码和数据均在 GitHub 上发布，对应地址为：https://github.com/duoergun0729/4book，代码层面任何疑问可以在 GitHub 上直接反馈。本书的写作时间主要集中在晚上十一点以后，难免会有错漏之处，恳请大家将发现的错别字和表述有误的地方反馈给我，我会在后面的版本中改正。

# 目 录

# 第1章

# 开源软件与网络安全

## 1.1 开源软件重大事件

### 1. 盘古开天地之 GNU 计划

1983 年 9 月 27 日，理查·斯托曼发起 GNU 计划，GNU 成就了开源和自由软件在今日的繁荣昌盛。1985 年理查·斯托曼又创立了自由软件基金会来为 GNU 计划提供技术、法律以及财政支持。随着时间的推移，GNU 计划产生了不计其数的开源软件，GNU 通用公共许可证（GPL）也随之诞生。这时候的 GNU 软件中就差一个 OS 内核尚未完成。1992 年 Linux 与其他 GNU 软件结合，完全自由的操作系统正式诞生。

### 2. 石破天惊之 Linux

1991 年的年初，林纳斯·托瓦兹开始在一台 386 兼容机上学习 minix 操作系统。

1991 年 4 月，林纳斯·托瓦兹开始酝酿并着手编制自己的操作系统。

1991 年 7 月，第一个与 Linux 有关的消息是在 comp.os.minix 上发布的。

1991 年的 10 月，林纳斯·托瓦兹在 comp.os.minix 新闻组上发布消息，正式向外宣布 Linux 内核的诞生。

1993 年，大约有 100 余名程序员参与了 Linux 内核代码编写工作，其中核心组

由 5 人组成，此时 Linux 0.99 的代码大约有十万行，用户大约有 10 万左右。也许当时谁也不会想到，Linux 会在未来的几十年深刻改变了世界[⊖]。

### 3. 雨后春笋

在 Linux 出现后的几十年里，各种开源软件如雨后春笋般出现，它们深刻改变着互联网的面貌。

1993 年，红帽成立；

1994 年，MySQL 启动；

1996 年，Apache 称霸互联网；

2005 年，Hadoop 横空出世；

2010 年，OpenStack 出现；

2015 年，TensorFlow 开始流行。

## 1.2　国内外安全形势

2016 年 4 月，CNCERT 监测发现一个名为“Ramnit”的网页恶意代码被挂载在境内近 600 个党政机关、企事业单位网站上，一旦用户访问网站就有可能受到挂马攻击，对网站访问用户的 PC 主机构成安全威胁（见图 1-1）。Ramnit 恶意代码是一个典型的 VBScript 蠕虫病毒，可通过网页挂马的方式进行传播，当用户浏览含有 Ramnit 恶意代码的 HTML 页面时，点击加载 ActiveX 控件，用户主机就很有可能受到恶意代码的感染[⊜]。

2016 年 5 月，俄罗斯黑客成功制造了一场大规模的数据泄露事故。在此次网络攻击中，黑客盗取了 2.723 亿个账号，以俄罗斯最受欢迎的电子邮件服务 Mail.ru 用户为主，此外还有 Gmail 地址、雅虎以及微软电邮 Hotmail 用户。路透社称，数以亿计的数据目前正在“俄罗斯的地下黑市”出售[⊝]。

⊖ http://wiki.mbalib.com/wiki/Linux

⊜ http://www.cnvd.org.cn/webinfo/show/3821

⊝ http://www.freebuf.com/news/103646.html