HZ BOOKS 华章IT

ELSEVIER 爱思唯尔

信息安全技术丛书

资深网络安全专家亲力打造，首部全面介绍情报先导信息安全方法和实践的著作

从威胁的种类、历史、特征入手，循序渐进地阐述如何实施情报先导的安全项目，结合内外部情报，拓展态势感知能力

防患未然

实施情报先导的信息安全方法与实践

[美] 艾伦·利斯卡 (Allan Liska) 著

姚军 吴冲华 译

机械工业出版社
China Machine Press

信息安全
技术丛书

防患未然

实施情报先导的信息安全方法与实践

[美] 艾伦·利斯卡 (Allan Liska) 著
姚军 吴冲华 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

防患未然：实施情报先导的信息安全方法与实践 /（美）利斯卡（Liska, A.）著；姚军，吴冲华译 . —北京：机械工业出版社，2016.1
（信息安全技术丛书）
书名原文：Building an Intelligence-Led Security Program

ISBN 978-7-111-52477-9

I. 防… II. ① 利… ② 姚… ③ 吴… 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（2015）第 309545 号

防患未然：实施情报先导的信息安全方法与实践

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：李　艺
责任校对：董纪丽
印　　刷：三河市宏图印务有限公司
版　　次：2016 年 1 月第 1 版第 1 次印刷
开　　本：147mm×210mm　1/32
印　　张：7
书　　号：ISBN 978-7-111-52477-9
定　　价：49.00 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

The Translator's Words 译者序

接受本次翻译邀请的时候，首先吸引我的是“情报”一词，这让身为军事迷的我浮想联翩，一度以为这是本讲述国家安全或者军事作战的书籍。

细读下来，书中大量引用了《孙子兵法》，再回想在IT行业这么多年的工作，网络安全工作也确实已经成为了一场“战争”：敌方的攻击行动已不再像过去那样从边界发动，而是层层渗透，利用各种社会工程手段侦察企业及人员情况，以钓鱼邮件等手段诱骗内部人员成为无意中的“帮凶”。更可怕的是，这种大大小小的“战役”发生的频度甚至超过了真正的战争，在大型企业中，每个雇员都成为入侵者的目标，他们每天接收到的钓鱼邮件，也许真能赶上战争时敌方打过来的炮弹数量了。

传统的网络防御三剑客——防火墙、入侵检测系统和桌面防病毒软件，已经不再能让我们高枕无忧，在敌人大打情报战的时候，我们该怎么办？只有以其人之道还治其人之身——实施情报先导的安全项目，结合内外部情报，拓展态势感知能力，先敌一步采取行动，将攻击扼杀在摇篮之中。

作为资深的网络安全专业人士，本书的作者Allan Liska以独到的视野，从威胁的种类、历史、特征入手，循序渐进地阐述了情

报的类型和重要性、网络安全情报模型、数据收集、内外部情报来源等情报先导安全项目中的重要概念及方法，为在各种网络攻击面前苦于招架的安全团队带来了一剂良药。虽然本书的篇幅不长，内涵却十分丰富。它不是泛泛地介绍各种工具，而是系统地介绍各种网络安全方法论，包括攻击链模型、网络安全情报模型、各种行业ISAC等组织的讲解，足以令读者茅塞顿开，在安全领域开辟新的道路。在翻译工作中，我们深深为书中丰富的思想方法、精彩讲解和实例所吸引，掩卷之时，衷心地向广大读者推荐本书，将其作为网络安全规划的重要参考。

本书的翻译工作主要由姚军、吴冲华完成，徐锋、陈志勇、刘建林、白龙、方翊、陈霞、林耀成、宁懿等也为翻译工作做出了贡献。由于译者水平所限，书中难免出现一些错误，请广大读者多加批评指正。在此也感谢机械工业出版社的编辑李艺和其他工作人员对翻译工作的大力支持。

Preface 前言

2015 年 2 月，我参加了 RSA 大会，这是我多年来第一次参加这项会议，会上我被网络安全领域在很短时间内发生的巨大变化深深打动。更确切地说，在很短的时间内，网络安全市场发生的巨大变化触动了我。

在 RSA 大会上，几乎每一家网络安全供应商都在兜售他们的情报，不管是供应商在平台中直接提供的原生情报，还是供应商与第三方情报提供上的集成。别误解，我坚信情报是在安全事故成为大问题之前识别和解决它们的最佳手段。但是情报不是一个数据摘要，也不是一系列指标。相反，情报是获得这些指标、使它们可以付诸行动，并提供指标背后威胁的来龙去脉的全过程。

实际上，编写本书的动机来自于 RSA 会议期间一个雨夜中与本书技术编辑 Tim Gallo 关于这一主题的一次交谈。本书不是关于系统配置的纯技术书籍，它的目标是帮助读者决定如何调整组织内部的安全过程，以容纳情报循环，并考虑所得情报的注入点。在使用得当的情况下，情报越好，给网络带来的保护越好。

本书是介绍这一复杂主题的第一次尝试，如果你愿意，可以把它称作版本 1.0。我十分感谢任何反馈，不管它们是正面的还是负面的，都可以帮助下一版本变得更好。你可以通过 allan@allan.org 和我联系，并提供任何意见。

致谢

本书的首要主题之一是信息共享的重要性。如果无法根据情报采取行动，或者情报没有及时交到需要根据它采取行动的人手中，那么情报就是毫无意义的。如果没有那么多网络威胁情报社区的人和我分享他们的知识，本书就不可能出版。

我要特别感谢一些人的帮助：Cisco 的 Brian Tillett，Carbon Black 的 Ben Johnson 和 Jeffrey Guy，CrowdStrike 的 Mike Cryer 和 Scott Fuselier，Palantir 的 Geoff Stowe，Symantec 的 Sean Murphy，Mandiant 的 Justin Bajko，Recorded Future 的 Jeson Hines，DomainTools 的 Tim Chen，Schweitzer Engineering Laboratories 的 Laura Scheweitzer，Reservoir Labs 的 Patrick Clancy，LockPath 的 Chris Goodwin 和 Chris Caldwell，ThreatConnect 的 Andy Pendergast 和 Michele Perry，eSentire 的 Sean Blenkhorn，以及 ThreatQuotient 的 Wayne Chiang。

我还要感谢 iSIGHT Partners 的同事们，感谢所有人在这段时间的支持。他们的支持、建议、想法和交流使我可以写出一本真正对广大读者有帮助的书。

除了广泛的社区支持之外，我还要感谢 Tim Gallo 出色的技术编辑工作。Tim 和我一起花费了很长的时间，提炼我们关于在组织中有效利用网络威胁情报的方法，因此，他对这本书的贡献和我一样多。实际上，本书中许多最巧妙的段落直接归功于他的编辑。

最后，如果没有 Syngress 的 Chris Katsaropoulos 和 Ben Rearick 的辛勤工作，本书就无法出版。感谢 Chris 相信我的想法并且帮助把它们转化成文字。感谢 Ben 帮我控制进度，在遇到阻力时鼓励我。他们两位使本书的出版过程比 10 年前轻松很多。

作者简介

Allan Liska 是 iSIGHT Partners 的技术联盟项目主管，是一位“事故”安全性专家。虽然 Allan 总是擅长破坏性的工作，但是他最早的专业工作是担任 Genie 在线服务（AOL 早期竞争者，已消亡多年）的客户服务代表，当时他将业余时间花在理解用户如何在未授权状态下访问系统、驱逐这些访问者并让开发人员知道需要打补丁的地方。在不知不觉中，这些工作使其走上了安全专家的道路。之后，他供职于 UUNET 和 Symantec 等公司，帮助各大公司加固网络安全。他还曾经在波音公司工作，尝试攻破公司的网络。今天，Allan 帮助各大公司实施情报工作，使所有安全设备相互通信，加大情报覆盖面。

除了将时间花在安全边界两端之外，Allan 还撰写了大量有关安全的书籍，包括《The Practice of Network Security》。此外，他还是《Apache Administrator's Handbook》的合著者。

技术编辑简介

Tim Gallo 是 Symantec 的现场工程师。他在 Symantec 有 11 年的工作经验，而在信息技术和 IT 安全方面已经有 16 年的经验。作为 Symantec 网络安全组的现场工程师，他为 Symantec 的客户提供策略和指导，帮助他们利用情报收集和传播建立具有前瞻性的保护方案。他还在其他方面为 Symantec 提供服务，包括 Symantec 情报服务的技术产品管理、全球服务与工程团队中的运营和交付任务，以及领导公司高级网络安全产品支持战略。在就职于 Symantec 之前，Tim 曾在一家领先的工业制造企业担任美国地区安全官员，负责战略性策略开发、测试和数据中心运营。作为当前工作的一部分，Tim 是安全策略、情报计划和威胁及安全漏洞管理领域的思想领袖。

目录 *Contents*

Chapter 1 第 1 章

理解威胁

1.1 引言

1981 年，伟大的 Jon Postel 在 RFC（请求注解）793 中写道："严以律己，宽以待人。" Postel 当时为美国国防部高级研究计划局（DARPA，1981）的互联网项目推出了传输控制协议（TCP）。TCP 是当今大部分互联网通信的基础，它的有效性正是因为上面的这段话，现在人们称之为 Postel 法则。对于互操作的多个网络系统来说，它们必须对接收的流量表现出宽容性，而在发送流量时则完全遵循确立的协议。Postel 法则还展示了互联网早期开发阶段所必需的思维方式。因为互联网通信相对新颖，必须尽可能地保持开放性。

正是这种开放性使互联网兴起，以至于今天许多用户和组织将互联网视为日常生活中必不可少的一部分。遗憾的是，这种开放性也意味着连接到互联网的系统容易遭到攻击。

这些攻击的性质和发展是本章的焦点。如果不首先理解这些攻击的来源以及它们多年来如何从科学研究变成成名的手段，甚至变成数十亿美元的生意，就不可能知道如何抵御今天和明天的攻击。威胁不断发展，解决方案也必须与时俱进。

1.2 网络安全简史

关于使用情报改善网络安全性这一课题的讨论必须从对网络安全历史的理解开始。毕竟，不了解过去以及安全威胁的演化，就难以理解网络安全的未来走向。

当今所称的“互联网”始于1982年由美国国防部信息系统局（DISA）和高级研究计划局（ARPA）发布的传输控制协议/互联网协议（TCP/IP）。根据Hobbes的《Internet Timeline》(Zakon, 2014)，这是第一次用“互联网”这个词定义一组相互连接的网络。

在那个时候，互联网非常小，主要由大学和政府机构组成，而且非常开放。要访问网络上的其他节点，运营商必须共享地址信息。每个运营商负责维护一张互联网上所有节点的表格，而且在情况变化时发送更新。

1.2.1 Morris 蠕虫

1988年11月2日Morris蠕虫（Seltzer，2013）的发布极大地改变了互联网的开放性。虽然在此之前已经出现过安全漏洞，但是Morris蠕虫还是引起了羽翼未丰的互联网对安全性的关注。

Morris蠕虫表面上用于对互联网上的节点进行统计调查，据估计它造成10%的节点下线（6000个节点，当时的网络估计有60 000个节点）。Morris蠕虫的使用的一些花招现在仍为蠕虫制作者采用，包括重定向（Morris在康奈尔大学，但是从麻省理工学院启动蠕虫）、密码猜测、自动填充和缓冲区溢出攻击。

不管意图是好是坏，Morris蠕虫的设计很明显是为了获得对互联网节点的未授权访问和绕过当时部署的不多的安全手段。Morris蠕虫直接导致了卡耐基·梅隆大学CERT协调中心（CERT/CC）的成立，这一组织至今仍然存在。Morris蠕虫还推进了第一种网络安全设施——防火墙的发展。

1.2.2 防火墙

和描述网络协议的许多术语一样，防火墙一词也来自物质世界。防火墙是用于减慢或者避免火势从一座房屋蔓延到另一座房屋或者从房屋的一部分蔓延到另一部分的建筑结构。它的目的是控制火势，将破坏限制在单一建筑物或者建筑物的一部分中。

大部分现代城市的房屋和公寓在相邻的单元之间都设置了防火墙，防火墙的规模还可能更大。1911 年 1 月的《 Brotherhood of Locomotive Firemen and Enginemen's Magazine 》(第 90 页）描述了从曼哈顿第 9 大街延伸到第 5 大道的防火墙。这个防火墙的建造是为了保护曼哈顿避免发生在巴尔的摩和旧金山的大规模火灾。

网络防火墙的最早期形式开发于 20 世纪 90 年代末，最初就是在路由器上增加了简单的包过滤规则。网关级别的包过滤使网络运营商可以阻止已知的“坏”流量进入网络，但是只能对安全性提供有限的改进。这些规则不仅难以维护，非常容易出现“误报”（即阻止实际上的“好”流量），而且需要大量的知识，了解组织中的每个人需要与谁通信、哪些通信对象需要阻止。包过滤在互联网很小、只包含 60 000 个节点的时候是理想的手段，但是网络的快速增长使其很快就不再实用，而需要新形式的防火墙。

下一种防火墙可以进行状态型包过滤，这类防火墙包括数字设备公司（DEC）和 AT&T 推出的第一批商用防火墙。状态型包过滤维护通过它的所有连接的一张表格，它的决策不仅根据流量的类型，而且根据两个主机之间连接的状态。状态型包过滤防火墙可以根据包的状态，以更基于上下文的方式决定流量的好坏，它实际上是商用网络安全市场的真正发端。从这时起，防火墙进入快速发展阶段，加入了代理、深度包检测、应用程序感知和 VPN（虚拟专用网）等功能。