HZ BOOKS
华章科技

绿盟科技——巨人背后的专家

在竞争激烈的互联网领域，总有一些组织和个人利用DDoS攻击进行破坏，从而达到自己的目的
本书为您揭晓互联网上最具破坏力、最难防御的攻击之一——DDoS

破坏之王

DDoS攻击与防范深度剖析

鲍旭华 洪海 曹志华◎著

NSFOCUS

机械工业出版社
China Machine Press

破坏之王

DDoS攻击与防范深度剖析

鲍旭华 洪海 曹志华◎著

机械工业出版社

图书在版编目（CIP）数据

破坏之王：DDoS 攻击与防范深度剖析 / 鲍旭华，洪海，曹志华著 . —北京：机械工业出版社，2014.4

ISBN 978-7-111-46283-5

Ⅰ. 破… Ⅱ. ①鲍… ②洪… ③曹… Ⅲ. 计算机网络 - 计算机安全 - 研究 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2014）第 062603 号

网际空间的发展带来了机遇，也带来了威胁，DDoS 是其中最具破坏力的攻击之一。本书从不同角度对 DDoS 进行了介绍，目的是从被攻击者的角度解答一些基本问题：谁在攻击我？攻击我的目的是什么？攻击者怎样进行攻击？我该如何保护自己？全书共分 7 章。第 1 章讲述了 DDoS 的发展历史，梳理了探索期、工具化、武器化和普及化的过程。第 2 章介绍了 DDoS 攻击的主要来源——僵尸网络，对于其发展、组建和危害进行了讨论，并专门介绍了自愿型僵尸网络。第 3 章讲解了 DDoS 的主要攻击方法，包括攻击网络带宽资源型、攻击系统资源型以及攻击应用资源型。第 4 章列举了攻击者使用的主要 DDoS 工具，对于综合性工具、压力测试工具和专业攻击工具分别举例详细介绍。第 5 章从攻击者的角度讨论了 DDoS 的成本和收益问题。第 6 章分析了 DDoS 的治理和缓解方法，对源头、路径和反射点的治理以及稀释和清洗技术进行了介绍。第 7 章展望未来，对网络战、APT 攻击和大数据技术进行了一些探讨。

本书适合各类人员阅读，信息安全专业的学生和爱好者、从事信息安全的咨询和运维人员、企业 IT 策略的制定者，都可以从中找到自己感兴趣的部分。

破坏之王——DDoS 攻击与防范深度剖析

鲍旭华 洪海 曹志华 著

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：王 彬

印 刷：北京瑞德印刷有限公司 版 次：2014 年 4 月第 1 版第 1 次印刷

开 本：186mm × 240mm 1/16 印 张：12.5

书 号：ISBN 978-7-111-46283-5 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）88378991 88361066 投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

序

随着科学技术的迅猛发展和深度应用，网络空间中的变革正在不断改变和影响着人们的生活方式。然而，一次次惊喜的背后，却隐藏着诸多隐患。无论是国家安全还是集体利益或个人利益，在网络空间中都会随时面临挑战。2013 年 8 月 25 日，我国顶级域名 CN 的解析服务器遭到攻击，造成大量以 cn 为后缀的网站无法访问，经济损失和社会影响难以估计。而导致这一严重后果的，就是分布式拒绝服务（Distributed Denial of Service，DDoS）攻击。

DDoS 是一种以破坏为目的的攻击，十几年来不断发展变化，成为不同组织和个人的工具，用于网络中的勒索、报复，甚至战争。从荒唐的“黑手党男孩”到神秘的“匿名人”组织，从雅虎、花旗这样的商业巨头到美国、俄罗斯、朝鲜与他国的争端，这本书揭示了 DDoS 的发展历史。

了解仅仅是开始，感兴趣的读者会有一系列疑问。谁在进行攻击？他们为什么发起攻击？使用了什么方法？如果我受到攻击，该怎样保护自己？这本书从多个角度对 DDoS 进行了解读。传统的 DDoS 大多来自僵尸网络，而近年来高性能服务器、移动设备甚至志愿者都成为了可能的来源；攻击者不是疯子，每次攻击都会有明确的目的，以及对成本和收益的考虑；DDoS 的原理看似繁杂，却可以归为三类，实用的工具则数不胜数；面对这种攻击，绝对的防御并不存在，综合五个环节的治理和缓解才是应对之道。最后，这本书在附录中还介绍了国外知名的黑客组织和个人，以及常见的几个误区。

本书的作者之一是我的学生。想不到在我心目中的孩子，转眼间有了自己的想法和见解，甚至都开始写书了。这本书称不上尽善尽美，很多观点也有可商榷处。但让我感到一丝欣慰的是，国内安全领域的一代新人正在成长。在我们的政府部门、学术机构和安全企业，有这么多当年熟悉的面孔，他们有了自己的思想和声音，不再盲目跟随国外的脚步。我能够感到，中国成为一个信息安全强国的日子，也许就在不远的将来。

冯登国

中国科学院软件研究所

2014 年 1 月 25 日

前　言

现实与网络中的战争

1939 年 9 月 1 日凌晨，第二次世界大战爆发。德军 14 个师兵分三路，从北、南、西同时入侵波兰，波军 6 个集团军 80 万人组成的防线瞬间瓦解。由于兵力分散和移动迟缓，波军很快被各个击破，到 9 月 21 日“布楚拉战役”结束，主力已全军覆没。这次战争的时间之短，出乎所有人的意料，它将一种新的战争模式呈现在人们眼前：“闪电战”。

人们在惊叹“闪电战”速度的同时，往往忽略了另一个因素：兵力对比。当时的德军的确强大，但波军也非弱旅，在之前的“波苏战争”中和苏联互有胜负。此外，德军的突击部队其实只有 14 个师，却能够轻易突破防线，还在之后的战斗中屡战屡胜，作用之大让当时的军事学家跌破眼镜。

2012 年 7 月，一部由美国制作的电影预告片被传到互联网上，由于包含对伊斯兰教的侮辱，引起了穆斯林的强烈抗议。9 月，一个自称“伊兹丁·哈桑网络战士”的黑客组织，在网上声称对美国金融业展开报复性战争。短短几周之中，美国银行、花旗集团、富国银行、美国合众银行、PNC 金融服务集团等金融巨头的网上服务因遭受攻击而中断，一个名字反复出现在报纸头条：“分布式拒绝服务攻击”。

一个名不见经传的黑客组织，面对这些金融巨头，为什么能一再获得胜利？成本高昂的防护系统，精英荟萃的安全团队，为什么不堪一击？到底什么是“分布式拒绝服务攻击”？

什么是分布式拒绝服务攻击

分布式拒绝服务攻击是从多个来源，彼此协同进行的拒绝服务攻击。这个名称包含了两层含义：首先，它是一种“拒绝服务”攻击；其次，它是一种“分布式”攻击。

那么，什么是“拒绝服务”（Denial of Service，DoS）呢？可以这样认为，凡是导致合法用户不

能访问服务的行为，就是“拒绝服务”攻击。最典型的例子是造成一个公开的网站无法访问。攻击者使用的方法通常很简单，就是不断提出服务请求，使服务提供方疲于应付，直到合法用户的请求来不及得到处理。

但是，大型企业或组织往往具有较强的服务提供能力，足以处理单个攻击者发起的所有请求。于是，攻击者会组织很多协作的同伴（或计算机），从不同的位置同时提出服务请求，直到服务无法被访问。这就是“分布式”。现实中，攻击者往往没有那么多同伴，所以，他们通常利用所谓的“僵尸网络”来控制大量计算机进行攻击。

然而，问题依然存在。为什么这种攻击具有如此威力？它和“闪电战”又有什么关系呢？笔者认为，这两者能够取得辉煌战果的根本原理是相同的：持续制造局部优势。

运用“闪电战”的德军，能够依靠机械化部队的速度集中兵力，每场战斗其实都是以强胜弱。波军则分散在漫长的国境上和广阔领土中，只能被各个击破，如果个别阵地存在顽强抵抗，德军就会绕过去，在另一个局部获得胜利。当失去友军支撑后，原本坚守的波军阵地只能不战而溃。所以，德军可以取得远超军力对比的战果。

网络世界中的一些特性有所变化。首先，IT 系统的依赖性更强，需要大量环境条件和其他应用来支撑，也就更容易存在弱点；其次，比起物理世界，攻击者可以提前观察受害目标，所以更容易发现弱点；再次，攻击者更方便组织攻击力量，完全让世界各地的被控制主机同时发起攻击。而“分布式拒绝服务”就是利用了这些特性。所以，即使拥有的资源、技术和人力远逊于专业团队，一个小型黑客组织也依然能够不断打垮金融巨头。原因无他，只因制造局部优势。

正如本杰明·萨瑟兰在他的《技术改变战争》中所述：“被视为‘非对称’的武器能够给予处于技术劣势的一方某种优势，让他们有机会去袭击装备更加先进的敌人。”

本书读者对象

DDoS 是一种破坏力很强的网络攻击方法，而且在可以预见的未来中，还没有任何手段能够完全防御这种攻击。本书希望从受攻击者的角度，来讨论以下几个问题：

1）谁在攻击我？

2）攻击我的目的是什么？

3）攻击者怎样进行攻击？

4）我该如何保护自己？

读者可能依然不了解自己是否有必要读这本书，那么可以试着回答以下问题，如果其中一个回答“是”，本书就可能会给你带来某种帮助。

1）我是否需要为公司（组织）的网络安全负责？

2）我是否需要为他人介绍一些基本的网络安全知识？

3）我的客户是否关心网络安全？

4）了解网络安全对我未来的职业发展是否有益？

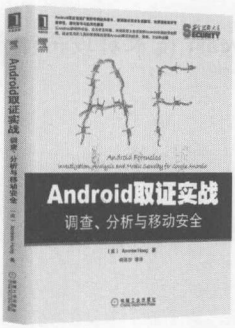
5）我管理的业务是否受安全基础设施的影响？

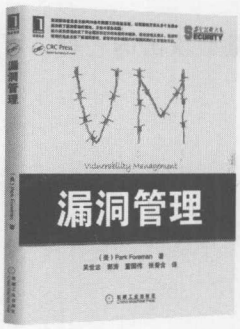
本书内容简介

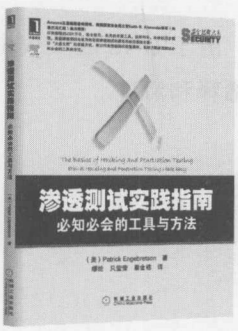
第 1 章讲述了 DDoS 的发展历史。第 2 章～第 4 章是本书的重点，从来源、方法和工具三个角度介绍 DDoS 攻击本身。第 5 章讨论攻击者的成本和收益问题。第 6 章分析在不同环节对 DDoS 的治理和缓解方法。第 7 章是对未来的一些探讨。

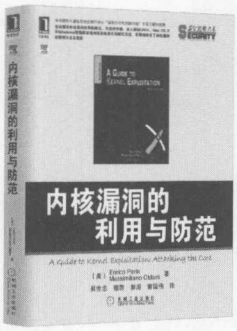
此外，本书在附录中提供了一些很有价值的资料。附录 A 是 DDoS 攻击方法、工具和相关事件的汇总；附录 B 解读了 9 个 DDoS 常见误区；附录 C 介绍了一些国外知名黑客组织和个人；附录 D 对 NTP 和 DNS 放大攻击做了更详细的解读；附录 E 提供了《2013 年绿盟科技 DDoS 威胁报告》，用真实数据说明 DDoS 攻击的现状。

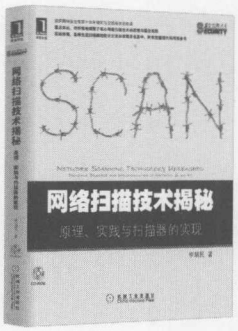
推荐阅读

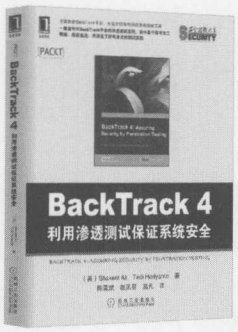












- **Android取证实战：调查、分析与移动安全**
  作者：Andrew hoog
  ISBN：978-7-111-42199-3
  定价：69.00元

- **漏洞管理**
  作者：Park Foreman
  ISBN：978-7-111-40137-7
  定价：69.00元

- **渗透测试实践指南：必知必会的工具与方法战**
  作者：Patrick Engebretson
  ISBN：978-7-111-40141-4
  定价：49.00元

- **内核漏洞的利用与防范**
  作者：Enrico Perla 等
  ISBN：978-7-111-37429-9
  定价：79.00元

- **网络扫描技术揭秘：原理、实践与扫描器的实现**
  作者：李瑞民
  ISBN：978-7-111-36532-7
  定价：79.00元

- **BackTrack 4: 利用渗透测试保证系统安全**
  作者：Shakeel Ali
  ISBN：978-7-111-36643-0
  定价：59.00元

目　录

第 1 章
DDoS 攻击的历史

“一切对存在的追问都以历史性为特征。”

——海德格尔

20 世纪的最后几年中，分布式拒绝服务（Distributed Denial of Service，DDoS）凭空出世，随后屡次在网络中掀起轩然大波，成为世界关注的焦点，即使对信息安全并不了解的人也耳熟能详。本章从历史的角度，为读者回顾这一过程。

关于“人类天生就具有攻击性”的命题是否正确，尚没有一个定论，也远远超出了本书的范畴。但是就历史来看，世界上的战争几乎从未停息过。而每当一种新技术诞生，就可能会被考虑是否可以用作武器。在物理学、化学、生物学、核物理学等领域，这样的例子不胜枚举。可被直接或间接用于实施攻击行为的技术，其发展和应用的历程存在一定的规律，一般而言，可以分为四个阶段。

1）**探索期：**新技术出现不久，人们不断摸索其使用方法，个人的兴趣和好奇心占主导地位。例如，火药出现后被用于制作爆竹。

2）**工具化：**技术的应用方式开始定型，成为实用性工具，对成本和收效的考虑占主导地位。例如，猎枪的出现以及火药在爆破领域的应用。

3）**武器化：**技术被大规模用于（或准备用于）战争中，政治势力会对该类武器的生产、拥有和使用进行控制。例如，大部分国家对现代枪械的管理方式。

4）**普及化：**技术的完善大幅降低了生产、使用和维护的成本，在法律允许的条件下，

个人拥有也变得容易。例如，美国允许公民拥有枪支，而拥有的成本很低，3D 打印的发展更是让技术门槛几乎消失。

不同技术的发展有各自的特点，其历程也会不同。例如核裂变技术，在经过了探索期后直接进入武器化，作为原子弹在战争中使用。之后才进入民用领域，出现了核电站。而随着原理的普及和成本下降，一位美国的 14 岁少年甚至自行制造出了核聚变反应堆，并在 TED 上发表演讲。[1] 不同的阶段之间也会存在重叠，同一技术很可能在军事领域和民用领域平行发展。

分布式拒绝服务攻击的发展符合这四个阶段。在探索期，发起攻击的“黑客”大多是一些技术爱好者，单纯为了兴趣或炫耀而进行了尝试，时间和目标的选择都很随意。随着工具化的发展，这项技术被用于有组织的行动，包括勒索、竞争或报复。为了使收益或效果最大化，他们会精确地选择目标和时机。当国家级政治势力意识到其价值时，分布式拒绝服务攻击很快被武器化，并用在网络战中。最后，随着使用越来越方便且易于获取，普及化也促进了黑客行动主义的发展。事件的爆发往往和群体的情绪有关，容易被外部事件触发，打击的范围开始扩大。与枪支和火药类似，分布式拒绝服务攻击也是平行发展的。表 1-1 列出了不同阶段 DDoS 攻击事件的特点。

表 1-1 不同阶段 DDoS 攻击事件的特点

时期	使用者	目的	时机	目标
探索期	“黑客”个体	兴趣和炫耀	随意	随意
工具化	政治、宗教、商业组织	勒索、竞争或报复	精确	精确
武器化	国家	网络战	精确	精确
普及化	群体组织	表达主张	受外部事件触发	相关范围

图 1-1 列出了在分布式拒绝服务攻击的发展历史中发生的主要攻击事件。本章的后续小节会分别详细介绍。

图 1-1 DDoS 的历史

1.1 探索期：个人黑客的攻击

早期的“黑客”都是一些技术爱好者。他们年轻、有激情、勇于探索，而且熟悉技术的最新进展，具有敏锐的洞察力。所以，他们能够找到当时系统中存在的漏洞和缺陷，并利用这些漏洞实现自己的目的。

“黑客”、“骇客”和“极客”的区别

“黑客”源自英文单词 hacker，原本在美国的电脑界是带有褒义的，特指那些擅长计算机技术，具有强烈的好奇心和动手能力，并且崇尚自由的人。早期的“黑客”都是高级程序员，他们发现系统中的漏洞，编写入侵工具，并实践它们。后来，一些虽不编写程序但擅长使用工具进行“实战”的人，也被纳入了“黑客”的范畴。他们善于通过蛛丝马迹寻找系统的弱点，选择合适的工具，来实现入侵的过程。

“骇客”是 Cracker 的音译，就是“破解者”的意思，本意是指那些专门破解商业软件，绕过付费机制，从而免费使用的人。很多“骇客”会将破解后的软件发布到互联网上供大众下载使用。后来，这一概念和“黑客”的概念被混淆了，两者的区别越来越模糊。

> “极客”来自于美国俚语Geek的音译，最初指性格古怪的人。很长时间，Geek在西方文化里一直偏向褒义。随着网络社交的普及，人们对“极客”的定义也逐渐发生了变化。现在，人们一般认为，花费大量业余时间在网络中，并且偏爱新技术产品的人群，就是“极客”。他们不一定是电脑高手，但对电脑和网络有很强的依赖性，喜欢尝试高科技产品。

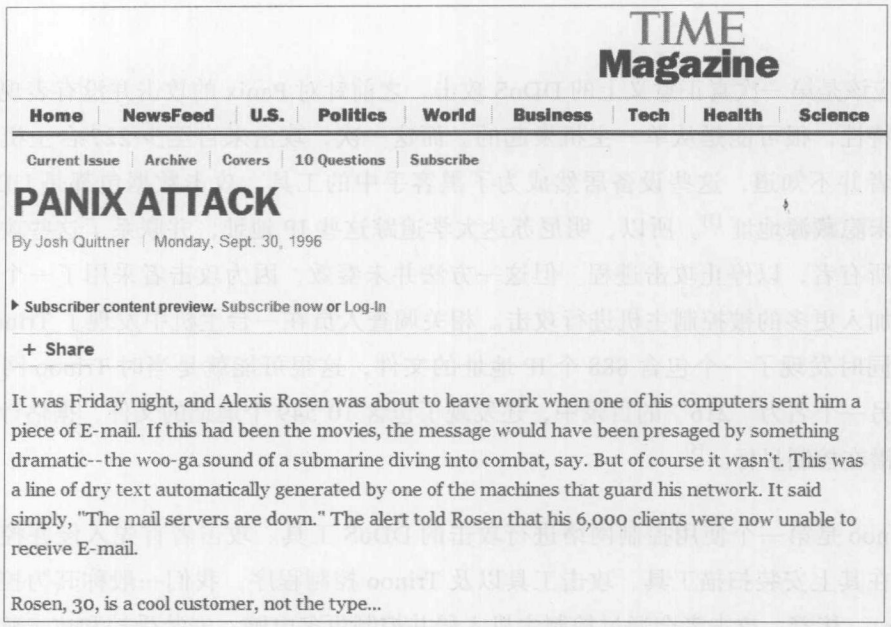
但同时，这些“黑客”在技术之外的领域并非天才。他们想到什么就做什么，随心所欲地发起攻击，而不是效力于特定组织。早期的分布式拒绝服务攻击往往缺乏明确的目的性，起因可能五花八门。也许是某人发现了一种有趣的攻击手法，只是想验证一下该攻击手法；也许是把攻击行为作为一种挑战，用以验证自己的天才能力；也许纯粹是为了向朋友炫耀。迈克尔·迪蒙·卡尔斯（“黑手党男孩”）甚至声称自己的目的是在网络世界中建立所谓“统治”。

所以，这些行为从攻击者的角度来看，基本不会带来经济上的收益。而从受害者的角度来看，往往波及的范围很大，具有轰动效果，但对具体的个人或组织，损失并非难以承受。

最早的拒绝服务攻击发生在1996年，受害者是当时纽约最大的互联网服务提供商Panix。3年后，发生了针对明尼苏达大学的攻击，攻击者使用Trinoo构建了真正的分布式控制网络。在早期的“黑客”行动中，最具轰动效应的就是“黑手党男孩”对雅虎、亚马逊等著名网站发动的攻击，这是早期“黑客”中暴露真实身份的一个。最著名可能也是最具威胁的一次，是2002年针对13台根域名服务器的攻击。虽然持续时间很短，也没有导致所有服务器完全瘫痪，但是只要设想一下行动成功的后果，就会让人不寒而栗。本节下面的内容就是对这几次事件的详细介绍。

1.1.1 第一次拒绝服务攻击

第一次拒绝服务攻击发生在1996年9月6日下午5:30。Panix，这个纽约市历史最悠久、规模最大的互联网服务提供商成为了攻击的受害者。公司的邮件、新闻、Web和域名服务器等同时遭受攻击。如图1-2所示，据《时代杂志》[2]（*Time Magazine*）报道，至少6000名用户因此而无法收取邮件。


TIME Magazine

Home | NewsFeed | U.S. | Politics | World | Business | Tech | Health | Science

Current Issue | Archive | Covers | 10 Questions | Subscribe

PANIX ATTACK

By Josh Quittner | Monday, Sept. 30, 1996

▸ Subscriber content preview. Subscribe now or Log-In

+ Share

It was Friday night, and Alexis Rosen was about to leave work when one of his computers sent him a piece of E-mail. If this had been the movies, the message would have been presaged by something dramatic--the woo-ga sound of a submarine diving into combat, say. But of course it wasn't. This was a line of dry text automatically generated by one of the machines that guard his network. It said simply, "The mail servers are down." The alert told Rosen that his 6,000 clients were now unable to receive E-mail.

Rosen, 30, is a cool customer, not the type...

图 1-2 Panix 攻击

攻击者采用的方法非常简单：不断向服务器发送连接请求（TCP SYN 请求），速度高达每秒 150 次。服务器忙于应对这些请求，从而无法回应正常的用户。这种攻击方式后来被称为“SYN FLOOD 攻击”，是拒绝服务攻击的一种。即使到现在，SYN FLOOD 攻击也经常被使用。此外，攻击者还采用了随机伪造源地址的方式。一方面，这使得攻击来源难以追踪；另一方面，随机的源地址也使得过滤和阻断攻击变得非常困难。[3]

完全消除 DDoS 攻击是极为困难的一件事。尤其当用户正常的访问量较大时，很难立刻将其与恶意伪造的访问区分开来。幸运的是，削弱这种攻击造成的危害是可能实现的。我们一般称其为“缓解技术”。Panix 被攻击后，计算机紧急响应小组（CERT）做出了快速响应。9 月 19 日发布了 TCP SYN Flooding and IP Spoofing Attacks，提出了缓解 SYN FLOOD 攻击和 IP 欺骗攻击的建议。[4]

1.1.2 分布式攻击网络：Trinoo

1999 年 8 月 17 日，美国明尼苏达大学的一台服务器遭到攻击，造成了连续两天的服务中止。接下来的几天中，又有至少 16 台主机遭到同样的攻击，其中有一些并不在美国