黑客大揭密

KNOW YOUR ENEMY

The Honeynet Project 著
曲向丽 潘莉 译

Addison Wesley

中国电力出版社
www.infopower.com.cn

黑客大揭密

KNOW YOUR ENEMY

The Honeynet Project 著
曲向丽 潘莉 译

中国电力出版社

内 容 提 要

本书是 Honeynet Project 两年研究的集体成果，出自世界一流的网络专家团体之手。本书共有三大部分：第一部分阐述 Honeynet 的规划、创建和维护，及其所涉及到的风险/问题；第二部分演示利用 Honeynet 的方法，以及如何从中学习，尤其是数据分析部分；第三部分包括几个破坏性 honeypot 的具体实例。本书深入浅出步骤翔实，无需太多的专业理论知识即可阅读。

本书适合网络安全方面的人员学习和研究之用。

图书在版编目（CIP）数据

黑客大揭密 / 美国蜜网工程著；曲向丽等译. —北京：中国电力出版社，2003

ISBN 7-5083-1490-5

Ⅰ.黑... Ⅱ.①美... ②曲... 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（2003）第 023091 号

著作权合同登记号 图字：01-2002-4839 号

本书英文版原名：Know Your Enemy

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.infopower.com.cn）

汇鑫印务有限公司印刷

各地新华书店经售

*

2003 年 7 月第一版 2003 年 7 月北京第一次印刷

787 毫米×1092 毫米 16 开本 15.25 印张 341 千字

定价 **32.00** 元

前　言

HONEYPOT 及 HONEYNET PROJECT

在战争中信息就是力量。对敌方了解得越深入，击败他的可能性就越大。在应对那些恶意黑客、网络入侵者及电脑世界里其他的 blackhat 们的反击战中，正义方手里所掌握的信息实在是少得可怜。大部分安全专家，甚至那些安全产品的设计者们，都忽视了敌方的工具、战略和动机。在这一点上，显然敌方是占优势的。

之所以发起成立 Honeynet Project，是希望能够藉此而燃起一些星星之火。这支研究队伍首先构建了一个完整的计算机网络，并用传感器对其进行了全副武装。然后他们就将其投入了 Internet，给它冠以一个比较恰当的、具有一定诱惑力的名字，同时也如法炮制了其所含的内容，并记录了其上所发生的活动。（实际的 IP 地址并未公布，并且该 IP 值也在定期地进行变更。）对黑客们的活动按照发生时的情形进行了记录：他们是怎样试着攻入系统的，他们是何时成功的，当他们成功之后又做了些什么。

结果非常有趣。Internet 上一台随机性的计算机一天会被扫描上许多次。生存期，或者说某人成功入侵前的持续时间，对于 Red Hat 6.2 服务器的默认安装来说要少于 72 小时。而对于常见的家庭用户设置，在 Windows 98 下再提供文件共享，在 4 天之内就会有 5 次被黑掉。平均每天系统被 NetBIOS 进行扫描的次数是 17 次。服务器被黑掉的最短时间记录为 15 分钟，从其连入网络后开始算起。

所有这些均说明了：每天都有惊人数目的人士试图闯入你的计算机网络，并且他们成功的概率也是相当惊人的。这是一场敌对性很强的战争，那些不采取积极防御措施的网络管理员很有可能就会被置于一种任人摆布的境地之中。

Honeynet Project 绝不仅仅是一个用来套人的计算机网络；它更是一个正在进行中的、对入侵黑客的操作方法学进行研究的项目。该工程目前已运行了若干个 honeynet。大家是否也想在自己的网络上尝试一下呢？目前已有几家公司在出售 Honeynet Project 的商业化版本，这些版本被进一步简化了。之所以称之为“honeypot”，是因为把它们设计成安装在某家组织的网络中充当诱饵。从理论上讲，黑客们会找到这些 honeypot 并在其上浪费时间，而实际的网络并不会因此而受到影响。

这似乎有点像是一个网络报警器。如果你在自己的网络中监测 24x7 警报，或者如果有一个受管理的安全监测服务，那么 honeypot 就能够在黑客发出攻击时予以响应，从而也就节省了宝贵的时间。当然，那些比较老练的攻击者也有可能会避过 honeypot。不过

在现实世界中，大多数的黑客都只是业余爱好者而已。这里的关键之处在于进行实时的监控，并在该项工作尚未较多实施的一周后查看一下日志文件。

为此，没有将其作为一个商品出售。Honeynet 和 honeypot 还需要加以呵护，它们不是那种可以进行自定义的产品。商业化的 honeypot 仅会模仿一个操作系统或者计算机网络，很难对它们进行正确的安装，并且相对于 Honeynet Project 的其他产品而言，要检测到它们的存在则要容易得多。同时它供给用户的安全保障也是增量式的。如果你确实对了解黑客及其工作方式感兴趣的话，不管怎样还是要买一个 honeypot 并要花些时间用好它。不过，如果你仅仅是对保护自己的网络感兴趣的话，那么最好还是将大部分时间用在其他事情上吧。

从另一方面来说，Honeynet Project 也纯粹是一项研究。而我本人就是一个主要的爱好者。它们所产生的东西都是无价的，也并没有什么其他的途径可以获取得到。如果有一架飞机在空中失事了，每个人都会知晓。因为有一项非常公开化的调查，任何一家航班的制造商都可以访问 National Traffic Safety Board 并阅读几百页关于所有近期飞机失事情况的报告。并且所有的航空公司都可以利用该信息来制造更好的飞机。但是，当网络被黑掉时，几乎大部分情况下都是一个谜。更为常见的是，牺牲者往往还不知道自己已经被黑了。即使知道了，由于来自市场方面的巨大压力，也不会将事实公布于众。而且即使公布了，几乎也不会给出那些细节性的情况，如黑客事件是怎样发生的及其后果如何等等。

而这些真实信息的缺乏，使得设计出优秀的安全产品变得更加困难。本书的主旨之一也正是希望能够改变这种境况。书中讲述了 Honeynet 的运作方式以及怎样去分析它所产生的数据，同时该书也综合了到目前为止它所学到的内容：“blackhat 社团”（即，恶意黑客）的工具、战略及动机。

本书适合于任何对计算机安全感兴趣的读者。素材丰富，而且真实可靠。

Bruce Schneier
http://www.counterpane.com

序

不知大家是否考虑过这样的问题：究竟是什么驱使着那些通常称作黑客的 blackhat 们去对系统进行攻击、破坏和捣鬼呢？一旦这些黑客们控制了系统，他们又会进行一些什么样的活动呢？这也正是本书的目的所在：教大家去了解这个敌人，即 blackhat。这些人总在试图利用 Internet 技术来进行一些非法的、破坏性的或者越权性的活动。这种活动的难易程度不等：简单的有诸如那些十几岁的青少年对网站的破坏企图，复杂的有诸如入侵信用卡公司，或者对某个国家的架构进行恐怖性攻击等。不管他们是谁（某个通过调制解调器进行链接的家庭用户，某家大组织的安全管理员，或者军队里的某位信息战官员），这些威胁都是确确实实存在着的。本书将会教给大家这些威胁背后的工具、战略以及动机：这样来了解你的敌人。

本书是 Honeynet Project 这个两年项目的结晶。这里所进行的研究，其与众不同之处就在于：让 blackhat 社团把他们的运作方式自己教出来，而没有试着去猜测究竟谁才是敌人，也没有根据 blackhat 的思考和操作方式来发展理论，而是让他们自己把其工具、战略和动机讲出来。学习的主要方法就是 Honeynet——一组旨在承受攻击的产品系统。当这些坏家伙们对这些系统进行探测、攻击和破坏时，就进行监视并从他们的每个步骤中进行学习。在过去的两年里，通过让各种系统被探测、攻击和破坏，我们也确实学到了很多东西。而也正是希望将这些所学共享出来，才有了本书的问世。此外，我们还创建了网站 http://projet.honeynet.org/book/，这个站点会包含所有与本书相关的附加信息，例如勘误、更新以及第 11 章中聊天会话的完整文本等。

对于那些没有技术背景的读者，本书将会用一些很简单的术语来演示这些坏蛋们是如何完成其破坏活动的。当然，要学习敌人的思考和操作方式，不必去了解所有的技术细节。我们也会教给大家一些很必要的技术技巧，以便对一次攻击进行研究并加以学习。而对于那些具备一定技术背景的读者，通过对数据的捕获和分析，如 forensic 分析，本书会进一步拓宽读者的技巧集。不过，不论原来的技巧集是怎样的，最终的目的都是相同的：告知大家我们从 blackhat 社团学到了什么以及是怎样学到的。我们真诚地希望：通过更好地了解敌人，大家也能更好地对攻击进行防护。

本书共有三大部分：在第一部分中，将会一步一步地告诉大家我们是怎样规划、创建和维护 Honeynet 的，及其所涉及到的风险/问题。在第二部分中，将会一步一步地向大家演示如何利用 Honeynet 以及如何从中学习，尤其是数据分析部分。在第三部分中，涉及了我们从 blackhat 社团所学到的内容，包括几个被破坏的 honeypot 的具体实例。在本书中，我们尽量做到少讨论理论，而主要关注于那些 blackhat 们的活动以及所得到的教

训。希望大家通过本书能够把我们从 blackhat 社团所学的内容都学到手。

致谢

这本书的独特之处在于：它绝非一项个人的工作，而是一组人的集体劳动成果：这个集体就是 Honeynet Project。这是一个由 30 名安全专家组成的小组，主旨在于了解 blackhat 社团并共享其所学到的内容。所有这些研究都是在他们自己的时间里、用他们自己的资源来进行的。通过该项研究使整个安全社团受益，这正是这个团队的真切希望。因此希望能够在这里占用一点时间，来对这些令人称道的专家们表示一下感谢。没有他们在时间上的付出和支持，无论是这项研究还是这本书，都是不可能问世的。在本书结尾，或者在 http://project.honeynet.org 网站上，大家可以对 Honeynet Project 的成员们做更多的了解。

没有安全社团其他人士的支持和贡献，也不可能完成这项研究。因此希望能够再占用一点时间来感谢一下这些成员。首先要感谢的是 FIRST 的 Roger Safian，感谢他所付出的时间，也感谢他对该项目的支持：从一开始，他就近乎疯狂地投入到该项目的合作中来了。还要感谢 SANS 的 Alan Paller：他对一个非常复杂的研究项目给出了关键性的指导。也十分感谢 Elias Levy、Alfred Huger、Ben Greenbaum 以及 securityfocus.com 的所有员工。他们是该项目及本书系列论文的第一支持者。还要感谢的是 Wietse Venema、Tan 和 Dan Farmer，感谢他们的辛勤工作，感谢他们帮忙开发了 forensic 分析功能和 Forensic Challenge。也要感谢 Pavle，感谢他自愿设计了我们的网站和 Honeynet 标志。同时还要感谢的是 Sean Brown，感谢他对本书的详细审读及其卓越的洞察力。Dave Wreski 和 linuxsecurity.com 的员工们一直以来都为本项目提供了出色的支持。还想感谢的是那些花时间审读本书的人，包括 Cory Scott、Char Sample、Howard Harkness、Marcus Leech 和 Richard Bejtlich。感谢本书的发行人员和各位编辑 Karen Gettman、Emily Frey、Elizabeth Ryan、Tracy Russ 以及 Addison-Wesley 的其他所有为本书的问世作出了贡献的员工们。本来和一位作者打交道就已经够麻烦了，而他们却要和三十位作者打交道。最后，当然绝非最不重要，我还想占用一点儿时间来感谢一下我的妻子 Ania，她的耐心以及对本书和本项目的理解都是永无止境的。

Lance Spitzner
Honeynet Project 的创始人

目　　录

第 3 部分　敌　　方

第1章

战　场

一位指挥官曾经告诉我，要击败敌人，首先必须要先了解敌人：他们的进攻方法、工具和战略及其目的所在。这条军事法则也完全适用于网络安全领域，灵验性恰如它在军事中的应用。在安全战中，blackhat 社团就是敌方：我们必须要防御这种威胁。不过，要赢得胜利，首先就必须要了解我们的这个敌人。

首次踏入网络安全这个领域时，我失望地发现：关于 blackhat 社团的信息实在是太匮乏了。的确，要找到一些关于 exploit、scanner 以及其他各种攻击工具的技术信息还是相当容易的。但是这些在整个安全领域里只不过扮演着一个很小的角色。我想知道更多的内容：攻击者们的目的何在？他们又试图获得什么？为什么？他们又是怎样识别出那些易受攻击的系统，然后进行捣鬼活动的？一旦攻击者们控制了系统又会发生什么？他们之间又是怎样互相通信的？我们要应付的是来自于单方的威胁还是多方的威胁？

这些问题中有很多在军事领域中会常常被问到。但是不同的是，在军事领域中我们可以找到问题的答案。有些特定的组织，通常称之为军事情报局，或者 S2，专门负责获取和传播敌方信息。而对敌人了解得越透彻，胜利的可能性就会越大。例如，作为一名坦克军官，就期望能够对敌人的装甲战略和能力有个较好的了解。也期望能够知晓敌人某个坦克工厂的技术构架。这样就可以进行坦克射程、速度以及性能方面的训练。同时我们还会去阅读一些关于敌方历史和政治结构方面的书籍。亲身体验所俘获的装备。这些信息对于防御威胁是相当关键的。知道了坦克的射程，就能够估计出何时敌军会开火以及我方回应的时间。知道了敌军坦克的速度，就能够知道请求炮兵火力支援的时间容限是多少。知道了敌军坦克的性能（它的火力速度）就能够估计出敌军每分钟可以对我方开火的次数及其命中率。通过亲自操纵一下所俘获的 T-72，就可以很好地了解坦克内部敌军的可见范围。所有这些信息，对于击败对手而言无疑都是相当关键的。信息掌握得越多，阻截和打败敌军的胜算就越大。

令人震惊的是，在网络安全领域此类情报竟然如此缺乏。几乎就找不到关于谁是敌人、它的攻击方式以及在此所涉及的动机或者策略的信息。安全社团大多都在关注 blackhat 社团所用的特定技术工具，或者防御中所用的工具，而并没有去关注其战略或者

动机。我想知道的是：blackhat 社团是如何识别及探测出那些易受攻击的系统的？一旦系统被攻入会发生什么？他们瞒着我们又从事了些什么活动？问题实在很多而答案又少得可怜，这确实让我咋舌。我的工作是对威胁（敌人）进行防御，而我却还不知道敌人是谁，更不用谈它的工具和技术了。我想知晓更多的信息，但是该怎样去获取呢？

人们花了几年时间才开发出一种解决方案。其实计划也很简单：让敌方将他们自己的工具、战略和动机传授给我们。如果 blackhat 们能够一步步地把其操作方式演示给我们，为什么还要去发展理论呢？而除此之外，没有什么其他的来源会比这更为可靠或完整的了。在军事上，一些人称此为战场情报，由此而搜集来自敌军的信息。在网络安全中，我们也可以如法炮制，让 blackhat 把他们的操作方式自己教出来。现在的问题在于，在还不知道战场何在的情况下，怎样去搜集战场的情报呢？

就我而言，1998 年的战场位于我妻子的餐室里。在那年之初，我拥有了第一条连往 Internet 的专线，这样无论何时，世界上的任何一个人都可以访问我家里的网络了。起初，我并不知道其安全隐患，也没有意识到在电脑的世界里一场战争正在激烈地进行着。幸运的是，在那个时候我搜索了一下防火墙日志，并发现了大量可疑的流量在探测我的网络。我决定要好好了解一下这些流量，为此我又搜索了很多关于 Internet 的论文。尽管技术信息获得了不少，但是其中绝大多数都集中于某些特定的 exploit 或者 exploit 中所用的工具，而对获得敌方情报的方式所知甚少。我想知道更多的东西，但又不能确定该怎么去做。后来我决定在自己的网络上放置一个产品系统，并密切监测该系统，然后静观其变。我的目的就是让 blackhat 们给我演示一下他们是怎样对系统进行探测、攻击和捣鬼的。我所用的是 Linux Red Hat 5.0（一个 UNIX 操作系统的版本）的默认安装，并将其链接到了开放的网络中。我也不知道该期待什么，甚至会不会有人发现这个系统都是未知数。如果真有人发现了，又要花多长时间呢？系统会被攻破吗？一旦攻入之后又会发生什么呢？所有这些都是我希望能够回答的问题，但是这个方案能够行得通吗？1999 年 2 月 25 日，我把该系统链入了自己的网络中。在十五分钟之内，我的系统就遭到了识别、探测和攻击。而在那时我还几乎一无所知，但是我脑中却已经冒出了一个主意。

从这次经历中我学到了很多东西，主要是如何避免构建一个这样的环境。在构建了系统之后，blackhat 很快就发现了一些失误之处，擦写了硬盘，并且是永久性的无法恢复。我丢失了很多本来是可以获得的宝贵数据，譬如 blackhat 的按键、工具包以及系统活动等。这次几乎没学到什么东西，但事实证明这些都是可以做到的。通过将产品系统放置到一个网络中，然后监测所有进出该系统的活动，就有可能知晓更多关于敌方的信息。

随着时间的推进，这个理念逐步形成了 Honeynet Project，有 30 位安全专家专门对 blackhat 的工具、战略和动机进行学习并共享他们的所学。这个小组的学习方法是：创建产品系统，然后监测所有进出该系统的活动。当系统被探测、攻击和捣鬼时，我们就捕获并分析所有的数据。在项目研究和开发过程中，大家都自愿贡献出时间和一些特有的技巧。通过将技巧和知识结合起来，我们对 blackhat 社团的了解成指数递增。然后，我们就将这些信息共享给安全社团。最终的目的也就是为了增加对敌人的了解。在这些知

识的武装下，我们和安全社团都能更好地防御 blackhat 社团了。我们的与众不同之处就在于尽可能多地与安全社团进行共享，并希望每个人都能从我们的研究中获益。了解敌方工作方式的人越多，系统就会越安全，而这会使每个人间接受益。

这个项目是于 1999 年 4 月非正式开始的。我在开发捕获 blackhat 活动的方法方面需要帮助，2 月被黑掉的系统就提出了开发更加全面、更加完善的数据捕获方法的需求。一旦获取了数据，还需要对其进行分析的帮助，因为我对网络和系统活动，如解码一个从网络捕获来的特定的 exploit，所知并不是很多，所以我请了很多这些方面的人士来帮忙。幸运的是，安全社团是由很多既敬业又热心的人们组成的。例如，Marty Roesch（在 Snort 的开发员）就向 IDS（intrusion detection system，入侵监测系统）中加入了新的功能模块来帮助我们的研究工作——在此，击键日志，被称作会话中断。Max Vision 一步步帮着应对复杂的 exploit 攻击，并基于 exploit 的网络签名对其进行解码。没有他们以及其他一些人士的帮助，就不可能有这个项目。

Honeynet 会捕获各种非正常的网络活动和 blackhat 活动。没有哪一个人能够知晓所有这些涉及到的问题。当我们意识到还需要大量的专家支持时，我们的小组也在继续发展壮大。过了第二年，随着更多人士的加盟，这个项目也顺其自然地成长了起来。在这个小组中，每位成员都具有关于本项目的独特技巧、经验和背景。但是，我们有一个共同的愿望：了解 blackhat 社团并共享所学的内容。我们并没有严密的组织，其中很多人还从未碰过面。我们会不定期地通过 e-mail 共享信息，以便改进 Honeynet 的概念或者解码一个特定的签名或者攻击。

在 2000 年 6 月所有这些发生了戏剧性的变化，那时一个 Solaris 2.6 的 honeypot 被一个有组织的 blackhat 小组攻入了，并使用我们的 honeypot 进行通信。在三周的时间内，我们捕获了他们所有的对话。要对所有这些活动进行追踪，需要整个小组的技术，包括对特定的 IRC（Internet relay chat，Internet 中继闲聊）配置进行解码，以及将乌尔都语翻译成英语等。结果，这次事件促使我们这个非正规的小组变成了一个有组织的项目组。

直到那时我们才把自己当成了一个有组织的小组。事实上，Honeynet Project 这个名字也是在最后几分钟才给定的，因为在发布自己的发现时总要对自己和所作的研究有个称呼。从那之后，这个小组就吸引了其他的一些成员，如关注 blackhat 行为的心理学家 Max Kilger 博士。我们还和各种国家性的及国际性的组织建立了联系。我们继续进行技术开发和研究，并且总是和安全社团共享所学的内容。这本书则代表了另一种共享信息的方式。

这个团队所使用的主要工具被称作 Honeynet，一个被设计来充当被攻击对象的网络。然后我们就可以知道谁是敌人及其运作方式了。进出 Honeynet 的各个数据包都会被捕获和加以分析。系统中的每项动作都被载入了日志并采取了相应的安全保障。这个项目的美妙之处就在于没有任何理论。blackhat 一步一步地向我们展示了在现实世界中他们是如何操作的。一旦获取了这些信息，就可以对数据进行审查，并更好地确定出敌方，明了其目的、动机及操作方法了。

在整本书中使用了术语 blackhat 来代表敌方，即攻击者。也有很多人使用了术语 hacker、cracker 或者其他的一些叫法。我们不希望卷入到究竟该用哪些词来定义哪些人的政治争论中去。这里的标准是使用术语 blackhat 来代表那些坏人（敌人）。敌人可以是男性，也可以是女性，可以是一个对公司不满的员工，可以是一个青少年，也可以是受过高级训练的间谍。很多情况下，往往都不会知道敌人的身份。但有时也能够识别出他（们），并且会发现在这里什么都是有可能的。不过，最常见的情况是惟一可赋予他们的身份只有 blackhat 这一术语。不管怎样，它就是指试图对某种资源进行未授权活动的个人或者实体。

贯穿本书始终的共同主题就是去了解敌方，即 blackhat 社团。在第 2 章、第 3 章和第 4 章中，将会向大家介绍 Honeynet Project 的主要学习工具——Honeynet。我们会讨论这些产品系统究竟是什么，它们的价值，创建、使用和维护它们的方法，以及所涉及的风险/问题。在第 5 章~第 8 章中，涉及了如何使用 Honeynet 来捕获 blackhat 活动以及随后对所捕获的数据进行分析。基于这种分析，就可以学习 blackhat 社团的工具、战略和动机了。这里的分析包括系统论证、包分析以及日志审查。在第 9 章~第 12 章中，从一些文档完善的攻击实例出发，回顾了一下从 blackhat 社团所学到的东西。采用的方法是一步一步地说明敌方的思考和行为方式。我们会尽可能少地讨论理论而主要专注于所学的内容。本书最终的目的是教会大家：

- Honeynet：Honeynet 究竟为何物，它对于安全社团的价值所在，Honeynet 的工作方式，以及所涉及的风险和问题。
- 分析：如何对所捕获的数据进行分析，并由此学习 blackhat 社团的工具、战略和动机。
- 敌方：从 blackhat 社团处所了解到的信息。

真心希望大家能够学到些东西，并且能够从本书获得一些乐趣，正如我们在过去几年里那样。

第1部分 HONEYNET

聪明的人懂得向敌人学习。

——Aristophanes

过去，如果向一位安全专家询问黑客的情况，那么最有可能获得的都是高度技术性的回答，其内容大多会关于各种 exploit 工具以及一些关于各种攻击者战略和动机的精心猜测。我们对 blackhat 社团的理解在传统意义上往往会局限于攻击者所用的工具，而很少去了解这些工具的使用方法，是谁在使用它们，或者为什么要使用它们。安全专家们可以很详细地向你解释最新的缓冲区溢出攻击是如何工作的，或者基于 Web 攻击的功能，但是如果让他们解释一下究竟是谁在攻击这些系统，为什么这些系统会被攻击，或者一旦某个系统被攻入之后将会发生什么时，他们往往很难做出回答。是的，我们的理解还停留在所用的 exploit 工具及敌方行动的一些理论上。

这种集中行为也是很容易理解的。在安全社团内部，大部分人都是高度技术性的。这项工作确实需要具备高度技术性的技巧集，以便能够更好地理解所涉及的技术并实现和解决掉这些技术问题。因为这是传统意义上我们理解得最好的地方，也就是最容易用这些技术术语理解到所存在威胁的地方。同样，惟一可以从中学习的证据也就是被攻入的系统本身，以及黑客们所留下的工具和所造成的损害。通常，安全专家惟一能够断定的，可能就是系统中哪种易受攻击性被利用了，及其潜在的利用方式。有时，blackhat 会将工具落在被攻入的系统中，但是这些往往都会被擦除掉，或者是很难理解的。并且，将各种活动和网络、系统以及应用程序放在一起，也很难分辨出哪些是正常的产品活动，而哪些是可疑的或者恶意的活动。

Honeynet Project 正是一种希望能够改变这种状况的尝试。其目的在于对 blackhat 社团作尽可能多的了解。我们不仅要学习他们的工具，还要学习他们的战略和动机。我们不仅希望知晓这些坏家伙们使用的是什么工具，还希望知晓怎样使用它们以及为什么使用它们。这就是 Honeynet 的初衷。Honeynet 的力量在于 blackhat 们自己将其工具、战略和动机传授给了我们。我们所进行的学习是以他们的行动而非理论为基础的。

第2章

何谓 Honeynet[1]

HONEYPOT

honeypot 的概念已经存在很多年了。简单点儿说，honeypot 就是专门设计来引诱攻击者进行攻击的系统。一旦被黑掉了，它们就可以用于各种用途，例如作为一种警报机制或者进行欺骗。honeypot 最初是由数位计算机安全方面的泰斗在几篇优秀论文中提到的：Cliff Stoll 的“Cukoo's egg”[2]，及 Steve Bellovin 和 Bill Cheswick 的“An Evening with Berferd”[3]。在这两个实例中，都使用了 jail 类型的技术来捕获入侵者的会话并详细监测了入侵者所从事的活动。honeypot 这个术语是后来才出现的，但是其目的相同：建立一个或更多个对网络入侵者具有一定吸引力的系统，并且还可以对所发生的活动进行较好程度的监测。通过监测来往于 honeypot 的活动，就能够识别出问题的所在，并能够合理地推断出入侵者的入侵方式，以及他们在攻入的系统中做了些什么。从传统意义上来说，honeypot 是与某个已有的产品系统相联的单独系统，其目的在于吸引攻击者。图 2-1 就演示了置于内部网络中的一个单独的物理系统。该系统就可以对很多系统或者易受攻击环节进行效仿。

目前存在着大量可以用来创建自己的 honeypot 的产品和解决方案，现有的选择包括：

- Fred Cohen 的 Deception 工具包（http://www.all.net/dtk/index.html）
- Cybercop Sting（http://www.pgp.com/products/cybercop-sting/default.asp）
- Recourse Mantrap（http://www.recourse.com/products/mantrap/trap.html）

所有这些应用程序，对何谓 honeypot 以及如何使用都有自己的解释。

---

1 更新信息：本章主要讲解 honeypot 和 Honeynet 技术的定义和价值。可以从新的站点得知更为详细的信息：http://www.tracking-hackers.com。

2 C.Stoll，《The Cuckoo's Egg:Tracking a Spy Through the Maze of Computer Espionage》（New York:Pocket Books,1990）。

3 http://www.securityfocus.com/data/library/berferd.ps。

例如，Deception 工具包，通常称之为 DTK，是一组用来模拟各种已知易受攻击环节的脚本集。在 DTK 中，所模拟的一个这样的易受攻击环节就是一个很古老的用于散发伪造密码文件的 Sendmail。然后就可以在一台主机系统上运行这些脚本，这样攻击者就会被这份伪造的密码文件所吸引，并花费大量的宝贵时间来破解这份并非真实的密码。这个工具包的目的就在于进行欺骗，不过它在预警和了解已知易受攻击环节方面也很出色。

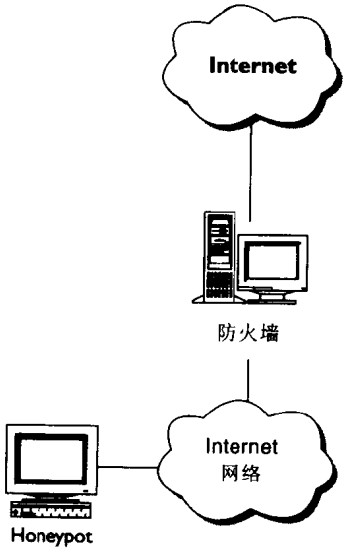

图 2-1 传统的单独 honeypot 系统

尽管这种方法是很有用的，不过要记住的是，Honeynet Project 的主要目的之一在于了解未知的易受攻击环节。如果使用 Deception 工具包，将会只限于了解到那些已知的内容。

Cybercop Sting 是一个运行于 NT 上的 honeypot，通过复制各种操作系统的 IP（Internet Protocol，IP 协议）栈来模拟整个网络。这样，当一个 blackhat 对全部网络进行扫描时，就会发现 15 个可利用的系统，而且每个系统都具有不同的 IP 地址。不过，实际上这 15 个虚拟系统全都驻留在同一台物理 honeypot 机器上。系统和 IP 栈都是模拟的。这里的好处在于可以迅速而简单地复制整个网络，从而对敌方的行动趋势进行追踪。但是，问题在于所能模拟的功能是有限的，例如 TELNET 登录或者 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）标识。blackhat 社团并没有什么实际的操作系统对超出的范围进行访问和交互。

我们希望学习到所有可能学习到的东西，譬如一旦系统被攻入后究竟会发生什么等。我们想知道他们的击键以及所侵入系统的系统日志。换句话说，我们希望攻击者能够完全利用和实现他们的目的，以便将来我们能够应对并学习到尽可能多的内容。鉴于其有限的模拟能力，类似于 Cybercop Sting 这样的产品是无法提供这类信息的。

Recourse Mantrap 是和 Honeynet 的功能很类似的一种商业产品，它并没有去复制一个操作系统，而是在一个操作系统中运行了另一个操作系统的映像。这种所谓的“jail”，其巨大的优越性在于确实有个真实的操作系统在运行。这样就可以知晓未知的薄弱环节