系统与安全丛书

PEARSON
Addison Wesley

honeypot：追踪黑客

Honeypots: Tracking Hackers

网络安全顶级专家教你如何追踪黑客

（美）Lance Spitzner 著
邓云佳 译

Pearson Education
清华大学出版社

系统与安全丛书

honeypot：追踪黑客

（美） Lance Spitzner 著
邓云佳 译

清华大学出版社
北京

内 容 简 介

本书深入讨论了追踪黑客的重要技术 honeypot。honeypot 的主要用意是通过部署虚假的主机来欺骗黑客、引诱黑客进行攻击、记录黑客的行为并阻止攻击泛滥。本书讨论了商用 honeypot、自制 honeypot 和 Honeynet，主要侧重于其运作方式、价值、实现方式及相应的优势。无论你是一名初学者还是有经验的安全专家，本书都是一种不可多得的资源。

本书适合本科生、技术人员、非技术人员、网络安全人员和网络系统管理员阅读。

EISBN: 0-321-10895-7

图书在版编目（CIP）数据

honeypot：追踪黑客/（美）施皮策（Spitzner, L.）著；邓云佳译．—北京：清华大学出版社，2004.9
（系统与安全丛书）
书名原文：Honeypots: Tracking Hackers
ISBN：7-302-09297-4
I. H... II. ①施... ②邓... 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（2004）第 086093 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969

文稿编辑：车立红　葛昊晗
封面设计：付剑飞
印 刷 者：北京四季青印刷厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：21.5　**字数**：430 千字
版　　次：2004 年 9 月第 1 版　2004 年 9 月第1 次印刷
书　　号：ISBN 7-302-09297-4/TP・6520
印　　数：1～4000
定　　价：39.00 元

序：以黑客之道还治黑客之身

我毫不掩饰自己是一个 Lance Spitzner 迷。这是一个电话留言为“我现在正忙着搞笑呢，请留言，我会尽快与你联系。”的家伙。我不知道何时他才会真正停止这种“搞笑”。有时我怀疑是否真有两个他。他对自己所从事活动的热情渗透到了其生活的方方面面。他那些酷酷的想法像火山像漩涡一样围绕着他，同时也吸引了旁观者和学生们。和他一起开会确实有些压力。有他在场，每个人都会显得很无趣，而且不够热情。Lance 热爱他所从事的事业，他的事业就是追踪黑客、共享该信息并且使其产生影响。

很多人喜欢称那些技术精英类的计算机爱好者为“黑客”——媒体人士则常常称其为“不可思议的神童”或类似的废话。Lance 使用 honeypot 和 Honeynet 的重要副产品之一是为我们提供了一幅更为清晰的活动中的黑客的视图：通常是一些技术上毫不高深的孩童，围着一些自己几乎不懂的技术转。在 *Know Your Enemy* 一书中，Honeynet Project 演示了大多数黑客是何其的活跃和拙劣。怎么，难道你不相信这一点？那么不妨就设置一个自己的 honeypot 或 Honeynet 并亲眼目睹一下吧。本书就提供了完成此项工作所需的工具和概念！

我认为对于安全界而言，Lance 撰写这本书真是太伟大了。过去，黑客们对其匿名性非常自信，他们无所顾忌地徜徉在我们的网络中，利用所攻破的系统放心地和其同伙聊天，或者对其他系统和站点启动攻击，并不担心会被检测到。然而，现在他们可能会停下来思考一下其操作基地是否安全——自己在策划攻击和玩弄花样时，实际上是否正处于被监视之下。

honeypot 将会成为追踪黑客的武器库中的一种关键武器。它们不仅能捕获到那些蹩脚的黑客，有时还能捕获到新工具，并能够让安全专家在它们广为扩散前迅速做出反应，从而降低其有效性。它们捕获的不仅仅是位于防火墙之外的脚本顽童，而且包括在公司任职的人（此时他们是黑客）。它们不仅能捕获不重要的人员，有时还会捕获到工业间谍。设置和操作 honeypot 可能耗时耗力，但是却很有趣，很有意义，并且是一个可以让人们在低风险的真实环境下获得计算机攻击培训的很好的途径。

现在市场上大约有十几种商用 honeypot 产品。Lance 在本书中讲述了其中的几种，同时还讨论了“自制”honeypot 和 Honeynet，主要侧重于其运作方式、价值、实现方式及其

相应的优势。我预测在一年的时间内会出现数十个商用 honeypot，在两年的时间内，数目会达到上百个。这对于我们而言都是好消息，因为这样我们就可以更轻松地部署 honeypot 了，而黑客或攻击者就更难识别和避开它们了。当你试图防御一种未知的新型攻击时，最好的防御就是一种未知形式的新防御。honeypot 会让黑客们保持警觉状态，并且我预计 honeypot 会做许多工作，来破坏攻击者们刀枪不入的感觉。本书非常适合作为了解当前可用的解决方案的入门书籍。

在本书中 Lance 也解决了围绕 honeypot 的合法性产生的一些疑惑。与我交谈过的很多执业者都害怕涉足 honeypot，因为他们害怕会被当成诱捕行动或者某种不法行为。你最好把关于法律问题的那一章读上两遍。它可能会让你大吃一惊。欢迎大家介入最新的一流技术，在这里创新不断发生，但还没有相应于新概念的法律。同时，随着对国家赞助的工业间谍和恐怖主义的重新关注，他们（big boy）也会设置自己的 honeypot。我讨厌成为一个选择从某个 CIA honeypot 系统启动下次攻击的脚本顽童！当这些人进入 honeypot 领域时，大家可以打赌他们肯定会确保其合法性。

可以将 honeypot 用于各种目的，甚至有用于垃圾邮件的 honeypot。你可以使用本书中的概念部署任何可以想像得出的 honeypot。你是否希望创建一个 honeypot 用于收集软件盗版？我认为这还不算完。那么通过追踪索引页面的点击率来测试哪种黑客工具最受欢迎的 honeypot 又如何呢？我认为这也不算完。可能性是无穷无尽的，并且我发现在阅读本书时很难不去反复地想“如果……那么会怎样？”。

希望你能够喜欢本书，并激发你发挥自己的创造性，了解黑客所从事的活动，然后与安全界共享。下面就跟着 Lance 的导引阅读本书，希望能对你产生影响。

Marcus J. Ranum
Woodbine, MD
2002 年 4 月

前　言

事情开始于一次无害的探测。一个奇怪的 IP 地址正在检查我的系统中的一项未用服务。在这个例子中，位于韩国的一台计算机正企图连接到我计算机上的一个 rpc 服务。没有任何理由有人想访问这项服务，尤其是位于韩国的某个人。肯定要出什么事情。紧随这次探测，我的入侵检测系统发出了一条预警：刚刚启动了一次漏洞攻击。我的系统遭受了袭击！攻击之后几秒钟，一位入侵者闯入了我的计算机，执行了几条命令，并完全控制了系统。我的计算机就这样被黑了！我真是兴高采烈！没有比这更让我高兴的了。

欢迎来到 honeypot 这个令人振奋的世界里，在这里我们可以反败为胜，捕获黑客。现在的大部分安全书籍都涉及了大量概念和技术，但是很多技术和概念都是将黑客拒之门外。本书则不同，它将黑客诱捕进来——关于如何创建希望被黑的计算机。从传统意义上说，安全一直是纯防御性的。组织很少能够掌握主动权并对攻击者发起挑战。honeypot 则改变了这条法则，这是一种容许组织发起进攻的技术。

honeypot 有各种形式和规模——从简单的模拟几项服务的 Windows 系统到等待被攻击的整个产品网络，不一而足。honeypot 还具有丰富的价值——从用于检测入侵者的警报机制到可用于研究黑客界动机的研究工具。honeypot 的独特之处在于：它们并不是一个解决某种特定问题的单独工具，而是一种高度灵活的可扮演很多不同角色的技术。所有的一切都取决于你希望如何使用和部署这些技术。

在本书中，我们解释了何谓 honeypot 和其运作方式，以及这种独特的技术所具有的不同价值。然后，我们详细讨论了 6 种不同的 honeypot 技术。我们分别解释了这些解决方案的工作方式、讨论了其优劣势所在，并演示了对各个 honeypot 的实际攻击会是什么样子。最后，我们讨论了 honeypot 的部署和维护问题。本书的目的不仅仅是让你理解 honeypot 的概念和构架，而且为你提供了部署最适合你的环境的 honeypot 方案的技能和经验。本书中的例子都基于现实中的经验，并且所讨论的几乎全部攻击实际上都发生了。大家可以看到黑客界的最佳表现和一些最糟的表现。最好的是，你能够用这些技能和知识武装自己，以追踪这些攻击者，并独立地了解他们。

多年来我一直在使用 honeypot，我发现它们绝对令人着迷。它们不愧为一种令人振奋

的技术，不仅可以教给你大量关于黑客的知识，而且还可以教给你关于自身和安全的一些概括性知识。希望读者能够喜欢本书，就像我喜欢编写关于 honeypot 技术的书籍，以及了解关于 honeypot 技术的情况一样。

读者对象

本书是为安全专家编写的。任何涉足于保护和安全加固计算机资源的人都会发现本书很有价值。这是第一本专门讲述 honeypot 技术的出版物，一旦了解了此种技术的能力和灵活性，就会有越来越多的计算机安全专家希望利用它。

由于 honeypot 的独特功能，其他个人和组织可能会对本书极感兴趣。军事组织可以将这些技术应用到计算机大战中。大学和安全研究组织会在关于研究型 honeypot 的材料中发现巨大的价值。情报机构可以将本书应用于情报和反情报活动中。法律执行机构的成员可以使用这份资料进行犯罪活动捕获。法律专家会发现第 15 章是第一个涉及 honeypot 法律问题的权威性资源。

网　　站

本书还有一个专有网站。网站的目的在于保持材料的更新。如果在书中发现了矛盾或者错误，网站就会进行更新和纠正。例如，如果本书中的任何 URL 发生了变化或者被删除了，网站都会提供更新后的链接。而且，新技术处于不断的开发和部署中。你应该定期访问网站，以了解最新的 honeypot 技术。

http://www.tracking-hackers.com/book/

参　　考

每一章都是以一个参考部分结束的。其目的在于为大家提供资源，用以获取与本书所讨论的话题相关的额外信息。参考的例子包括主要对操作系统进行安全加固的网站和专门进行攻击分析的书籍。

网　络　图

本书提供了用来演示 honeypot 部署的网络图。这些图给出了部署在网络环境中的产品系统和 honeypot。所有的产品系统和 honeypot 都是标准化的，因此可以很容易将它们区分开来。所有的产品系统都是简单的黑白计算机对象，如图 A 所示。这些就是你不希望被黑的系统。

与此相对，所有的 honeypot 都可以通过系统中所加的阴影和斜线很容易地识别出来，如图 B 所示。

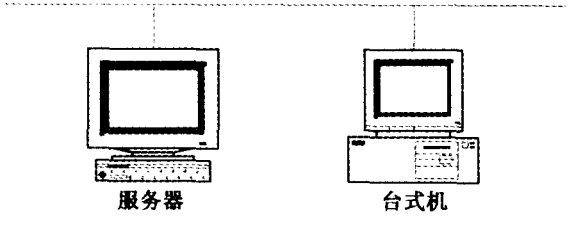

图 A　部署在一个网络中的两个产品系统

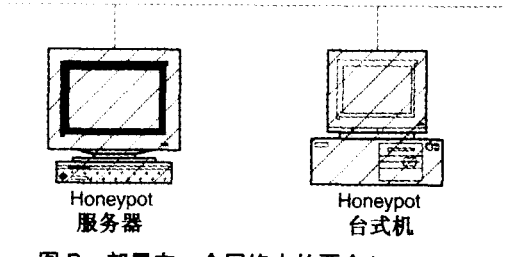

图 B　部署在一个网络中的两个 honeypot

目　录

第 1 章　刺激：我对 honeypot 的着迷

J4ck 兴奋极了，因为他刚刚获得了一个功能强大的新型黑客工具。有了这个工具，他就可以在整个世界范围内攻击并摧毁大量系统，即使没有数千个也有数百个。这的确会成为一个令人异常激动的夜晚。如果今晚他能够“黑”入足够多的计算机，他就可以证明自己是何其“精干”了。J4ck 知道大多数地下黑客都认为他只是个初出茅庐的新手。如果能够“黑掉”尽可能多的计算机，就可以向他们证明，自己其实要比他们所想像的高明多了。

J4ck 刚刚和他的黑客小组成员之一 J1ll 从 IRC（Internet Relay Chat）的聊天中离开。IRC 是一种在线聊天机制，它允许 J4ck 在 Internet 上即时地与世界各地的黑客伙伴们聊天。这与大部分公司目前所采用的电话会议颇有几分相似，只不过 IRC 是免费的。使用 IRC 只需要与 Internet 连接。IRC 还能够使人们通过 Internet 交换文件，如 exploit 程序和攻击代码。J4ck 起初就是通过 IRC 学习了大部分的攻击技术。他可以进入不同的聊天室，通常称之为“信道”（channel），在那里他会与形形色色的人相遇并发现最新的 exploit 程序。总是会发现新攻击以及一些脆弱点，IRC 就是一种即时发布该信息的有效途径。

IRC 也是 J4ck 今晚想攻入尽可能多的系统的另一个原因。因为他控制的系统越多，他的 BOT 值就越大。BOT，即 short for robot，是一种安装在被黑的计算机上的自动程序。这些 BOT 在 IRC 信道上维护了一个虚拟现场，执行攻击者编写的任何指令。J4ck 攻入的计算机越多，他可以部署的 BOT 就会越多。而他部署的 BOT 越多，他对 IRC 信道的控制就会越强。攻击者们总是试图将对方从 IRC 上踢出去——比如，敌对的双方可以发动一场拒绝服务攻击。J4ck 必须保护自己免遭攻击，然后再为攻击做好准备。这是 Internet 上的一场计算机大战，并且今晚他攻下的计算机数越多，他的武器库就会越强大。

J1ll 刚刚向他解释了如何使用这个新的 rpc.statd exploit 程序，利用它可以获得对那些运行 rpc.statd 并且尚未打补丁的 Linux 服务器的访问权。Linux 是在世界范围内使用的 Unix 操作系统的一种极为常见的形式。真是不可思议！成千上万的此类计算机乖乖地候在那里等待攻击。J1ll 还传送了这个新型 exploit 程序的已编译好的版本。J4ck 惟一的顾虑就是他获得的是该工具的一个预编译版本而不是源代码。这就意味着他不能在二进制码中检查出任何恶意代码。他不相信计算机世界里其他的大部分黑客：他们对攻击自己的同类抱有与

攻击 Internet 上其他任何人相同的兴趣。

这一点提醒了他：如果他获得了最新的 Linux rootkit 就太好了。rootkit 是一种工具包，设计用于在计算机被黑时对其进行重新编程。它们可以执行大量功能，包括清除系统日志文件、实现后门、向各种文件甚至所运行的内核中植入木马。一旦计算机被重新编程，它就会向管理员撒谎。系统管理员可能会“询问”计算机是否遭受了攻击或者被摧毁，计算机会谎称没有遭到攻击。而且，此时被重新编程的计算机在系统中已经被植入了后门，这样攻击者就有很多途径可以进入系统。

和许多黑客相同，J4ck 拥有一些用来对被黑系统打补丁和进行安全加固的工具。J4ck 知道，如果他不对刚刚攻下的计算机进行安全加固，他的同伙或者其他的攻击者就会发现这个系统并摧毁它。这些人一直都在那里和自己一样进行着主动扫描和攻击。J4ck 不能信任同伙，所以只能对系统进行安全加固来防止他们侵入。

J4ck 并不知道这种新型的 rpc.statd exploit 程序是怎样运作的——他所知道的仅限于那些用来运行该工具的命令。不过，他需要知道的就是这些。他已经拿到了一份很容易修改的旧 exploit 程序脚本。该脚本一旦运行，就会以准备攻击的网络作为输入，然后再将这部分信息传给实际的 exploit 程序。要使新的 exploit 程序运行起来，J4ck 只需先拿到脚本，然后将旧 exploit 程序的名字换成新 rpc.statd exploit 程序的名字。每当发布了新 exploit 程序时，他都会重复这一过程。脚本会代替他执行其他的工作，比如扫描并黑入脆弱系统，当系统被摧毁后上传 rootkit，对被攻击系统进行重新编程，并维护一份记录成功摧毁全部系统的日志文件。

一旦更新了他的脚本，整个过程就相当简单了。由于该工具是完全自动的，因此他要做的工作仅仅是将工具集上传到一台已被自己黑掉的计算机中，启动工具，几个小时后再回来看看工具已经进入了什么系统。实际上，J4ck 从没有使用过自己的计算机来攻击其他的计算机或者与其 h4x0r 伙伴（h4x0r 是一种术语，用于指代具备一定技术实力的黑客，是“hacker”的俚语表述）进行通信。J4ck 感谢 J1ll 为他提供了新工具，他停止了活动，然后带着一丝阴笑开始用新武器对整个国家展开攻击。

上面描述的并非什么科幻小说：它确确实实在发生着。这两个攻击者的每一步动作、每一次对话都被捕获并记录了下来。他们的姓名和身份被隐去了，但他们的活动却是真实的。J4ck 和 J1ll 未曾意识到的是：他们的一举一动都被一组安全专家进行了监视和捕获，因为他们攻入的一个计算机是 honeypot。刺激开始了[1]！

1.1　honeypot 的诱惑

自第一次听说了 honeypot 这个概念后，我就迷上了这项技术。honeypot 与大部分传统的安全机制有很大不同。这是一种安全资源，其价值在被探测、攻击或者攻破时体现。创建并部署一台旨在被攻击的计算机的想法很神秘，并且也很刺激。初次听说 honeypot 时，我正在一家总部位于芝加哥的咨询公司担任系统管理员的工作。某个深夜，我和几个同事正在进行文件服务器的重建工作，这台服务器由于硬盘错误不停地崩溃。在那个深夜的几个小时对话中，我们的一位高级管理员提到了 honeypot 的思路。当时由于初涉安全领域，因此以前还从未听说过这样的想法——“想要”被黑掉的一台计算机。太令人兴奋了！听起来似乎像是某种类型的间谍电影，CIA 特工渗透到了外国，了解敌方最为重要和最为隐蔽的机密。我一下子就被吸引住了，只想知道得更多一些。

这个概念令人兴奋的地方是扭转了和攻击者之间的形势。一直以来，我们很难了解黑客攻击、侵入及接管某台计算机的秘密。类似于其他形式的犯罪，攻击者们如何进行操作、使用何种工具、如何学会攻击以及他们攻击的动机何在，所有这些我们都知之甚少。honeypot 为我们开启了窥视这个世界的一扇窗户。通过监视攻击者侵入和控制 honeypot 的过程，我们就可以知道这些人是如何进行操作的及其原因所在。

honeypot 还为我们提供了另一个优势：进攻的能力。从传统意义上说，主动权往往都掌握在攻击者手中。他们控制着攻击的对象、时间和方式。在安全界所能做的只有防御：制定安全措施、防止攻击者进入，然后随时检测这些预防措施是否失效。正如任何一位优秀的军事家将会告诉你的，良好的防御就是良好的进攻。但是计算机世界的安全人员如何才能取得主动权呢？安全管理员不可能去随机攻击每个探测过他们的系统，这样做的结果只能是让 Internet 崩溃，更不用说所涉及的责任问题了。组织往往会受限于如何发动对攻击者的战争。也正是因为这个问题，我才对 honeypot 如此感兴趣。它们通过交给我们控制权赋予了我们相当的优势：允许攻击者对它们进行攻击。也正是因为诸如此类的一些问题，我才会迫不及待地投入进来并开始使用 honeypot。

我是在 1999 年开始和 honeypot 打交道的，并且很快就发现关于如何创建和使用它们的信息实在是太少了。相对于诸如加密、防火墙和入侵检测系统——关于它们正在撰写或者已经撰写了很多著作——之类的安全工具而言，对 honeypot 进行定义的文档实在少得可怜。因此，我判定了解什么是 honeypot 的最佳方法就是亲手创建一个 honeypot，制造大量问题，并从这些错误中学习（出错可是我的强项）。

1.2 我是如何开始和 honeypot 打交道的

那么，怎样创建 honeypot 呢？没有任何文档的好处之一是至少可以保证我不会出错。因为不存在任何规则说明 honeypot 应该是什么或者应该像什么样子，这样对于我所做的每种尝试，其方向都是正确的。

我的研究始于那时仅有的一个公共可用的 honeypot：Fred Cohen 的 The Deception Toolkit[2]。这是一组用 Perl 和 C 编写的工具包，它对大量服务进行了模拟。它安装在一个 Unix 系统上，通常称作 DTK，用于对攻击进行检测和欺骗攻击者。我试了试 DTK，发现它对于初次开启 honeypot 之门是极其有用的。不过，我也发现了其局限性：它仅仅模拟了一些已知的脆弱点，并且所提供的信息量也极为有限。在使用 DTK 时，并没有攻击者可以与之交互的操作系统——只是模拟服务。这样就限制了所能收集到的有关攻击者的信息。然而，DTK 确确实实激发了我的兴趣。

接下来，我尝试了另一个 honeypot 解决方案：CyberCop Sting，这是首批为组织开发的商用 honeypot 之一。我碰巧认识该产品最初的开发人员 Alfred Huger，这样我就得到了一份评测版产品。这套解决方案给我留下的印象是：易于部署并且可同时模拟多种系统。只需将 CyberCop Sting 安装在 Windows NT 系统上，在一份简单的文件中对几个选项进行配置，就可以让它运行了。这样就立刻得到了一个配备了各种 Linux、Solaris 和 NT 系统的网络。单独一个 honeypot 就可以模拟出一个完整的计算机网络。然而，我再一次发现了 CyberCop Sting 的局限性：攻击者们只能连接到某些特定的端口并读到相应的标识（banner）。例如，他们可以 Telnet 到一个模拟系统，比如 Solaris，并获得一个登录标识。然后攻击者可能会不断地进行登录尝试，每次尝试都会被 honeypot 记入日志。然而，攻击者永远都不会获得访问权，因为并没有一个确实存在的操作系统可供他们访问。这种模拟服务只允许登录尝试，这样一来交互性就大打折扣了。我感兴趣的是了解攻击者是如何进行操作的，所以我需要一个确实可以进行交互的 honeypot。

在这种情况下，我萌生了开发一个可以模拟各种服务的 honeypot 的想法。它类似于 DTK：honeypot 可以与攻击者进行交互；而且它也类似于 CyberCop Sting：不同的 honeypot 同时存在。我在寻找这样一种系统，它集这两方面的优点于一身：一种具备多个系统的高级别交互。

遗憾的是，我遇到了两个问题：（1）我相当不耐心，（2）我不喜欢写代码。如果我要亲自编写模拟各种服务的 honeypot 的代码，则需要投入大量工作，并且结果很有可能会是一次痛苦的失败。没有耐心加上缺乏编码技术迫使我去考虑另一个解决方案：不是模拟系