<<虚拟蜜罐>>

图书基本信息

书名：<<虚拟蜜罐>>

13位ISBN编号：9787508480169

10位ISBN编号：7508480163

出版时间：2011-1

出版时间：中国水利水电出版社

作者：Niels Provos,Thorsten Holz

页数：310

译者：张浩军,李景峰

<<虚拟蜜罐>>

前言

这是一本通过实验理解计算机安全的书。
在此之前，你可能会认为，如果你的计算机被攻陷了，那就是世界末日了。
但是，我们将告诉你如何看待入侵的光明的一面，教会你欣赏从僵尸网络、蠕虫和恶意软件中获得的知识。
每一次事件都会获得一个经验，一旦你了解了许多不同种类的蜜罐，在对付互联网攻击者时，你就可以反败为胜。
本书讨论了各种各样的蜜罐部署方案，从追踪僵尸网络到捕获恶意软件。
我们也鼓励你通过分析攻击者如何着手检测你的对策，从而获得敌手的视角。
但首先让我们建立适当的讨论环境。
计算机网络连接了世界各地无数的计算机系统。
我们知道，所有这些网络的总和构成了互联网。
互联网最初设计用于研究和军事目的，自从Tim Berners-Lee在1990年发明了超文本传输协议（HTTP）并创建了万维网之后，互联网变得非常流行。
随着我们中多数人开始使用网络，几乎所有的社会问题也转移到电子王国。
例如，由于人们的好奇心创造了第一个互联网蠕虫。
另一个好奇心的标志是扫描网络——扫描网络中安装计算机的数量和它们各自的配置。
事实上，接收一个持续的网络探测流现在被认为是正常的和所期望的。
不幸的是，许多这样的活动不再是良性的了。
社会中不良的人已经明白了互联网提供了快速获得利益的新机会。
地下活动从发送数以百万计的垃圾电子邮件、身份盗窃、信用卡诈骗，到利用分布式拒绝服务攻击进行敲诈勒索。
随着互联网的日益普及，保持我们的电子世界的健康运转也变得越来越重要。
然而，尽管有几十年的研究和经验，我们仍然无法保障计算机系统安全，哪怕是衡量他们的安全性。
利用新发现的漏洞的攻击往往使我们感到吃惊。
漏洞利用的自动化和大规模全面扫描漏洞，使得敌手一旦找到了计算机系统的弱点，就很容易攻陷计算机系统。
为了了解哪些漏洞正在被对手使用（它们甚至可能是一些我们尚不知道的），我们可以在网络上安装一个计算机系统，然后观察在它上面会发生什么事情.如果系统服务没有用于任何其他目的，那么任何一个对它的连接尝试似乎都是可疑的。
如果系统受到攻击，我们就可以了解某些新的东西。
我们称这样一个系统为蜜罐，它被攻陷能让我们了解入侵利用了哪个漏洞，一旦敌手掌握了对系统完全控制权后他做了什么。
一个蜜罐可以是任何类型的计算系统，它可以运行任何操作系统和任何数量的服务。
我们配置的服务决定了对敌手公开的攻击向量。

<<虚拟蜜罐>>

内容概要

本书全面而详细地介绍蜜罐技术的概念、分类及应用，及低交互蜜罐、高交互蜜罐、混合蜜罐，以及客户端蜜罐的实现机理与部署应用方式。
书中结合具体的工具，尤其是开源工具，阐述各类蜜罐的建立、配置和应用，介绍蜜罐在恶意软件捕获、僵尸网络追踪中的应用，并通过案例分析，结合实际讨论蜜罐的作用与应用效果。

<<虚拟蜜罐>>

作者简介

作者：（美国）普罗沃斯（Niels Provos） （美国）霍尔兹（Thorsten Holz） 译者：李景峰 等 合著者：张浩军Niels Provos，谷歌高级工程师，他开发了Honeyd蜜罐系统——一个开源的虚拟蜜罐系统，这个系统获得了Network World颁发的最高发明奖，他还是OpenSSH的创建者之一，他获得了汉堡大学数学博士学位，密歇根大学计算机科学与工程学博士学位。
Thorsten Holz，德国曼海姆大学分布式系统可靠性实验室博士生，他是德国蜜网项目的奠基者之一，也是蜜网研究联盟指导委员会成员。

<<虚拟蜜罐>>

书籍目录

<<虚拟蜜罐>>

章节摘录

插图：高交互蜜罐的缺点之一是较高的维护量：你必须小心监测你的蜜罐，并密切观察所发生的事情，分析危险还需要一些时间，从我们的经验来看，分析一个完整的事件可能花费数小时甚至数天，直到你完全明白攻击者想干什么！
高交互蜜罐可以完全被攻陷，它们运行着带有所有漏洞的真实的操作系统，没有使用仿真，攻击者可以与真实的系统和真实的服务交互，允许我们捕获大量的威胁信息。
当攻击者获得非授权访问时，我们可以捕捉他们的漏洞利用，监视他们的按键，找到他们的工具，或者搞清他们的动机。
高交互解决方案的缺点是它们增加了风险：由于攻击者可能完全地访问操作系统，他们就有可能用它来损害其他非蜜罐系统。

媒体关注与评论

这是当今最好的蜜罐技术参考资料，从低交互蜜罐，到僵尸网络，再到恶意软件，Niels Provos和Tborstea Hoiz通过本书，分享了他们在网络安全尖端领域之专业的知识、深刻的见解，以及令人叹为以止的才智。
如果您想学习最新的蜜罐技术，了解它们到底是什么、如何工作以及它到底能为您带来什么，至少是现在，没有比这本书更好的了。
——蜜网项目创始人Lances Spitzner Provos和Holz写的这本书，坏家伙们肯定不希望你们阅读。然而，任何对网络安全技术持有严肃态度的人，书架上绝不会没有这本书。
——Aviel D.Rubin，博士，约翰霍普金斯大学计算机科学教授，信息安全研究所技术总监，独立安全评估公司创始人和总裁 “ 专业、见解深刻并充满才智的一本书，为读者揭开了蜜罐世界的面纱，” ——Lenny Zeltser, Gemini系统公司信息安全业务部负责人 “ 这是本年度必读的安全书籍之一。” ——Cyrus Peiukari, Airscanner移动安全公司CEO《安全卫生》一书的作者 “ 无疑这是蜜罐领域最具权威的著作之一，它内容全面，文笔流畅，作者从-个行家的视角来审视虚拟蜜罐，帮助我们建立和理解原本很复杂的技术，” ——Stufan Kelm, Secorvo安全顾问 “ 无论是收集用于研究和防御的信息，还是隔离企业内部爆发的恶意软件，或者出于兴趣在家里观察黑客活动，在这本书里你会发现很多实际的骗术，展现了蜜罐的神奇！” ——Dugsong，Arbor网络首席安全架构师 “ Provos和Holz写的这本书，坏家伙们不希望你们阅读，对蜜罐详实而全面的讨论为我们提供了一步一步的指示——抓住攻击者的破绽，识破他们的把戏，并哄骗他们对安全产生一种错觉，不管你是一个从业者、一个教育工作者或是一名学生，这本书提供了大量的有价值的东西，本书涵盖了蜜罐的基本理论，但主要内容还是指导你如何做——建立蜜罐，配置它们，最有效地使用陷阱，同时保持实际系统的安全，自从发明防火墙以来，还没有一个像它一样有用的工具，在无休止的攻防竞赛中为安全专家提供了保护计算机系统安全的优势，《虚拟蜜罐》是一本必读书，应放在任何认真对待安全问题的人的书架上，” ——Aviel D.Rubin，博士，约翰霍普金斯大学计算机科学教授，信息安全研究所技术总监，独立安全评估公司创始人和总裁

<<虚拟蜜罐>>

编辑推荐

《虚拟蜜罐:从僵尸网络追踪到入侵检测》：蜜罐技术已经为网络安全做出了巨大贡献，但物理蜜罐部署的复杂、耗时及昂贵，却常常令人对它望而却步。
现在有了一个突破性的解决方案——虚拟蜜罐技术。
它具有物理蜜罐技术的诸多特性，但却使你可以在单一的系统中运行成百上千个虚拟蜜罐，同时，虚拟蜜罐的搭建比物理蜜罐更加容易，成本更低，更加易于部署和维护。
在这本可实践性极强的书中，两位世界上最重要的蜜罐技术先驱——Provos和Holz，为大家系统地讲解了虚拟蜜罐技术。
哪怕你以前从来都没有部署过一个蜜罐系统，通过《虚拟蜜罐:从僵尸网络追踪到入侵检测》，你也将会一步一个脚印地在自己的计算机环境中，准确掌握如何部署、配置、使用和维护虚拟蜜罐系统。
《虚拟蜜罐:从僵尸网络追踪到入侵检测》的学习将通过一个完整的虚拟蜜罐系统——H0oneyd为案例来进行。
这个系统由《虚拟蜜罐:从僵尸网络追踪到入侵检测》作者之一Pr0V0s创建，是一个专业领域内好评如潮的虚拟蜜罐系统。
同时，作者还为虚拟蜜罐系统准备了多个实际中使用的应用程序，如网络诱饵、蠕虫探测、垃圾邮件阻止、网络模拟。
对比高交互蜜罐(真实的系统及服务)与低交互蜜罐(用来模拟高交互蜜罐)。
安装与配置蜜罐，模拟多操作系统、应用及网络环境。
使用虚拟蜜罐来捕获蠕虫、僵尸以及其他恶意软件。
使用低交互蜜罐和高交互蜜罐中的技术，生成高性能混合型蜜罐。
在客户端部署蜜罐技术来主动发现危险的网络定位。
掌握攻击者如何识别和规避蜜罐。
解析蜜罐系统定位的网络僵尸及捕获的恶意软件。
预测物理蜜罐及虚拟蜜罐的进化趋势。

版权说明