<<灰帽黑客>>

图书基本信息

书名：<<灰帽黑客>>

13位ISBN编号：9787302301509

10位ISBN编号：7302301506

出版时间：2012-11

出版时间：清华大学出版社

作者：[美]Allen Harper,[美]Shon Harris

页数：586

字数：895000

译者：杨明军,韩智文,程文俊

前言

我已经受够了一场战争，更别提再来一场了。
——托马斯·杰弗逊　　我不知道第三次世界大战的武器会是什么样子。但我知道第四次世界大战战场上用的肯定是棍棒与石头。
——阿尔伯特·爱因斯坦　　兵法非常简单。找出敌人在哪里，尽快到达那里，尽可能凶狠地打击他，而且要挺住。
——尤利西斯·S·格兰特　　本书的目标是帮助培养更多技术精湛的、专注于抵御恶意黑客攻击的安全专家。事实一再证明，对敌方的了解是非常重要的，包括他们的策略、技能、工具和动机。企业和国家所面临的敌手非常专注，而且技艺超群。我们必须携起手来才能理解敌方的行动过程和流程，以确保我们能够正确地挫败敌方具有破坏性的恶意攻击。

本书的作者希望为读者提供他们认为这个行业所需的信息，即对负责任的而且在意图和物质方面真正合乎道德标准的正义黑客技术的整体性讨论。这也是为什么本书一开始就给出正义黑客的定义的原因所在，社会上对正义黑客的理解是非常模糊的。

本书对前两版中的材料进行了更新，并尝试将最全面、最新的技术、流程和材料汇集起来。因此增加了9章全新的内容，同时对其他章的内容进行了新新。

本书第Ⅰ部分制定了灰帽黑客必要的伦理和期望基础。该部分内容包括：理清人们对白帽、黑帽和灰帽黑客的定义和特征的混淆认识 讨论在实施任何类型的正义黑客行动前应该了解的一些棘手的道德问题 讨论漏洞发现报告的难点以及可用于解决这些难题的一些模型 调查黑客攻击以及许多其他类型的恶意行为所涉及的法律问题 概览适当的漏洞发现流程以及当前提供指导方向的模型。

第Ⅱ部分介绍了现如今其他书籍中没有讲到的更高级的渗透测试方法和工具。现在的许多书籍讲的都是一些相同的、被无数次反复翻新的旧的工具和方法，而本书决定更加深入地讲解真正的灰帽黑客正在使用的高级机制。该部分我们讨论如下内容：　　用来实施渗透测试的自动化渗透测试方法和高级工具 最新的渗透测试工具潜入攻击、社会工程以及内部攻击。

第Ⅲ部分将深入底层代码，向读者讲解各种操作系统和应用程序的特定部件的工作原理以及如何对它们加以利用。该部分将讨论如下内容：　　介绍一些基本的编程知识，这些是理解剩余内容所需要掌握的概念　　如何利用栈操作漏洞以及如何识别和编写缓冲区溢出攻击代码　　如何识别高级的Linux和Windows漏洞以及如何对它们加以利用　　如何创建不同类型的shellcode来开发自己的概念验证漏洞攻击程序和必要的软件，以测试和识别漏洞　　.最新的攻击类型，包括基于客户端的、Web服务器、VoIP以及SCADA攻击　　第Ⅳ部分将更深入地研究正义黑客技术的最高级主题，甚至当今的许多安全专家都没有理解这些主题。该部分将讨论如下内容：　　被动和主动分析工具和方法　　如何识别源代码和二进制文件中的漏洞　　如何进行软件的逆向工程和组件的反汇编　　模糊处理和调试技术　　如何为二进制和源代码打补丁　　第Ⅴ部分将讲解恶意软件分析。有时候正义黑客会遇到恶意软件，而且可能需要进行一些基本的分析。该部分将讨论如下内容：　　收集恶意软件样本　　分析恶意软件，包括对反模糊处理技术进行讨论。

如果您希望进一步提高和加深对正义黑客技术的了解，那么本书非常适合您。

<<灰帽黑客>>

内容概要

运用最新技术查找和修复安全漏洞，得力地阻止恶意的网络入侵。《灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)》在上一版本的基础上做了全面细致的更新，共新增了9章精彩内容：详细介绍了最新的安全漏洞和补救措施以及法定披露方式，分析黑客们如何定位目标系统、击破保护方案、编写恶意代码以及利用windows和linux系统中的缺陷，还探讨了恶意软件分析、渗透测试、scada、网络电话和web安全等方面的内容。

《灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)》主要内容
使用backtrack和metasploit来模拟漏洞攻击
分析潜入、社交工程和内部攻击技术
模拟构建用来发起栈缓冲区溢出攻击的perl、python和ruby脚本
理解并阻止adobe、office和多媒体文件中的恶意内容
检测和阻止客户端、web服务器、voip和scada攻击
介绍针对windows和linux软件的逆向工程、模糊处理及反编译
讨论sql注入、跨站脚本和伪造攻击
使用蜜罐和沙箱技术来捕获恶意软件和rootkit

作者简介

作者：（美国）哈珀（Allen Harper） （美国）哈里斯（Shon Harris） 译者：杨明军 韩智文 程文俊 哈珀（Allen Harper），CISSP，曾任美国财政部、国税局计算机安全应急响应中心的安全分析师，现任N2NetSecurity公司总裁Allen经常在Black HatChrechno等会议上发表演讲。
哈里斯（Shon Harris），CISSP，Logical Security总裁、作家、教育工作者、安全顾问。
Shon已经发表多篇著作和论文，Information Security Magazine杂志将她评为信息安全领域最杰出的25位女性之一。

书籍目录

章节摘录

当发现bug后，他们希望供应商立即发布修复措施。
这确实是一把双刃剑。
但是，供应商经常采取的“渗透并修补”的做法招致了安全社区的指责，因为供应商仅仅是发布多个临时性的修复措施来安抚用户，从而避免自己的声誉受损。
安全专家称，这种临时方法不是一种良好的工程实践。
大多数安全缺陷发生在应用程序设计过程的早期。
应用程序的优劣可以通过6个关键的因素区分：身份验证和授权 最好的应用程序应能保证身份验证和授权步骤是完善的，并且不能被绕开。
不信任用户输入 应该将用户当做“敌方代理”，在服务器端验证数据，并通过去掉字符串的标记来防止缓冲区溢出。
端到端会话加密 应该加密整个会话，而不是只加密活动中包含敏感信息的部分。
另外，安全的应用程序的超时时限应该较短，如果用户有一段时间不活动，那么在再次使用应用程序时需要重新进行身份验证。
安全的数据处理 安全的应用程序还将保证系统处于不活动状态时数据是安全的。
例如，口令存储在数据库中时仍然应该是加密的，而且应该实现安全的数据隔离机制。
不恰当地实现加密组件常常为敏感数据的未授权访问提供了很多机会。
消除不当配置、后门和默认设置 许多软件供应商的一种常见但不安全的做法是销售带有后门、实用工具和管理功能的软件，以帮助接收信息的管理员了解和使用该产品，问题在于，这类增强通常会包含严重的安全缺陷。
因此应该总是禁用这些选项，用户可以在需要时再启用它们，并且所有的后门都应该从源代码中恰当地清除。
安全质量保证 设计产品时，无论是在规范制定和开发阶段，还是在测试阶段，安全性都应该是一个核心的关注点。
因此，供应商应该组建安全质量保证团队（security quality assurance team，SQA）来管理所有与安全相关的问题。
2.7 接下来应该处理的事项 我们可以通过完成一些活动来改进当前的安全状况，但是该过程中涉及的每个人都应该更具有前瞻性、接受过良好的培训并具有更大的动力。
如果确实想让自己的环境更加安全，那么就应该遵循下面列出的一些惯例：积极行动 确保环境安全不只是开发人员的责任，同时也是用户的责任，用户应该积极查阅有关安全功能的文档，并向供应商索取测试结果。
许多安全问题就是因为用户配置不当造成的。
培训应用程序开发人员 经过良好培训的开发人员可以创建更安全的产品。
供应商应该在安全领域认真地培训他们的雇员。

媒体关注与评论

如果您是一名渗透测试人员或研究人员，而且希望快速地提高和拓宽自己的IT安全技能，那么本书将是您的良师益友。

——Corelan Team创始人Peter Van Eeckhoutte（corelanc0d3r）

编辑推荐

《灰帽黑客:正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)》是由清华大学出版社出版。

名人推荐

“一本面向渗透测试者和研究员的优秀参考书，将帮助他们在广阔的信息安全领域提高和扩展技巧。”——Corelan Team创始人Peter Van EeCkhoutte(corelancOd3r)

版权说明