

<<黑客之道>>

图书基本信息

书名：<<黑客之道>>

13位ISBN编号：9787508426983

10位ISBN编号：7508426983

出版时间：2005-3-1

出版时间：中国水利水电出版社

作者：Jon Erickson,范书义,田玉敏

页数：193

字数：284000

译者：范书义,田玉敏

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<黑客之道>>

### 内容概要

黑客攻击是一门创造性的艺术。

《黑客之道：漏洞发掘的艺术》带您进入黑客的世界，为您讲解每一个真正的黑客必须具备的坚实的技术基础。

本书详细介绍了黑客攻击的理论及其精贿，以及支持黑客进行攻击的科学，同时探讨了一些具体示例，包括：利用缓冲区溢出和格式化字符串的漏洞编写攻击程序；编写可打印ASCII多态shellcode；TCP连接；利用FMS攻击揭开加密的802.11b无线流。

通过这些示例教您学习黑客攻击的一些核心技术和技巧，理解黑客的思想和习惯。

一旦您掌握了黑客攻击的思路，您就可以早作防范，提前发掘系统或者网路的漏洞，防止潜在攻击。

本书主要面向广大计算机安全与网络安全爱好者，只要您想精通黑客攻击技术，无论您是想攻击还是想防御，本书都值得您一读。

## <<黑客之道>>

### 作者简介

Jon Erickson，受过计算机科学的正规教育，经常在国际计算机安全会议上发表演讲。他目前是北加利福尼亚密码学和安全方面的专家。

## 书籍目录

前言第1章 绪论第2章 程序设计 2.1 什么是程序设计 2.2 漏洞入侵程序 2.3 通用exploit技巧 2.4 多用户文件权限 2.5 存储器 2.5.1 存储声明 2.5.2 零字节结束符 2.5.3 程序存储器的分段 2.6 缓冲区溢出 2.7 基于堆栈的溢出 2.7.1 不和漏洞检测代码入侵程序 2.7.2 利用环境 2.8 基于堆和bss的溢出 2.8.1 一种基本的基于堆的溢出 2.8.2 函数指针溢出 2.9 格式化字符串 2.9.1 格式化字符串和printf() 2.9.2 格式化字符串的漏洞 2.9.3 读取任意存储地址的内容 2.9.4 向任意存储地址写入 2.9.5 直接参数存取 2.9.6 用dtors间接修改 2.9.7 重写全局偏移表 2.10 编写shellcode 2.10.1 常用汇编指令 2.10.2 linux系统调用 2.10.3 Hello,world! 2.10.4 shell-spawning代码 2.10.5 避免使用其他的段 2.10.6 删除空字节 2.10.7 使用堆栈的更小shellcode 2.10.8 可打印的ASCII指令 2.10.9 多态shellcode 2.10.10 可打印的ASCII多态shellcode 2.10.11 Disembler 2.11 returning into libc 2.11.1 returning into system() 2.11.2 链接returning into libc调用 2.11.3 使用包装器 2.11.4 用returning into libc空字节 2.11.5 一次调用写入多个字第3章 网络 3.1 什么是网络互连 3.2 关键层详述 3.2.1 网络层 3.2.2 传输层 3.2.3 数据链路层 3.3 网络窃听 3.4 TCP/IP劫持 3.5 拒绝服务 3.5.1 死亡之ping 3.5.2 泪滴 3.5.3 ping淹没 3.5.4 放大攻击 3.5.5 分布式Dos淹没 3.5.6 SYN淹没 3.6 端口扫描 3.6.1 秘密SYN扫描 3.6.2 FIN、X-mas和Null扫描 3.6.3 欺骗诱饵 3.6.4 空闲扫描 3.6.5 主动防御第4章 密码学第5章 结束语参考文献

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>