

<<网络渗透技术>>

图书基本信息

书名：<<网络渗透技术>>

13位ISBN编号：9787121010354

10位ISBN编号：7121010356

出版时间：2005-1

出版时间：电子工业出版社

作者：许治坤等

页数：676

字数：1000000

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>

## <<网络渗透技术>>

### 内容概要

《网络渗透技术》是国内第一本全面深入地披露系统与网络底层安全技术的书籍。本书分为十个章节，详细介绍了渗透测试技术的方方面面。

首先介绍了各种调试器和分析工具的简单使用，然后从各种操作系统的体系结构讲起，深入浅出地分析了相应平台的缓冲区溢出利用技术，接着介绍其高级shellcode技术，以及更深入的堆溢出利用技术等。

除了用户层的利用技术，在第6章还以Linux操作系统为例详细地介绍了内核溢出的各种利用技术。另外还结合实例，详细介绍了类UNIX系统漏洞分析与发掘技术。

本书不放过每一处技术细节，记录了分析调试过程的每一个步骤，并且给出详细的演示程序。在最后两个章节，本书还对渗透测试撕裂口——Web应用的渗透做了精辟的描述。

本书是XFOCUS团队倾力之作，对于有志于网络安全事业人士而言，本书是一本不可多得的专业参考书。

## 书籍目录

第1章 基础知识 1.1 GDB的基本使用方法 1.1.1 断点相关命令 1.1.2 执行相关命令 1.1.3 信息查看相关命令 1.1.4 其他常用命令 1.1.5 Insight图形界面调试器 1.2 SoftICE的基本使用方法 1.2.1 断点相关命令 1.2.2 执行相关命令 1.2.3 查看与修改相关命令 1.2.4 其他常用命令 1.2.5 常用默认快捷键 1.3 NTSD (WinDbg/CDB)的基本使用方法 1.3.1 断点相关命令 1.3.2 执行相关命令 1.3.3 查看与修改相关命令 1.3.4 其他常用命令 1.4 IDA Pro的基本使用方法 1.4.1 强大的反汇编功能 1.4.2 方便的代码阅读功能 1.4.3 常用默认快捷键第2章 缓冲区溢出利用技术 2.1 缓冲区溢出历史 2.2 Linux x86平台缓冲区溢出利用技术 2.2.1 Linux的内存管理 2.2.2 缓冲区溢出的流程 2.2.3 缓冲区溢出的攻击技术 2.3 Win32平台缓冲区溢出利用技术 2.3.1 Win32平台缓冲区溢出的流程 2.3.2 跳转地址 2.3.3 远程缓冲区溢出演示 2.3.4 结构化异常处理 2.3.5 Windows XP和2003下的增强异常处理 2.3.6 突破Windows 2003堆栈保护 2.4 AIX PowerPC平台缓冲区溢出利用技术 2.4.1 熟悉PowerPC体系及其精简指令集计算 2.4.2 AIX PowerPC堆栈结构 2.4.3 学习如何攻击AIX PowerPC的溢出程序 2.5 Solaris SPARC平台缓冲区溢出利用技术 2.5.1 SPARC体系结构 2.5.2 Solaris SPARC堆栈结构及函数调用过程 2.5.3 学习如何攻击Solaris SPARC的溢出程序 2.6 HP-UX PA平台缓冲区溢出利用技术 2.6.1 PA-RISC体系结构 2.6.2 常用指令集 2.6.3 运行时体系结构(Run ~ time Architecture) 2.6.4 学习如何攻击HP-UX下的溢出程序 2.7 Windows CE缓冲区溢出利用技术 2.7.1 ARM简介 2.7.2 Windows CE内存管理 2.7.3 Windows CE的进程和线程 2.7.4 Windows CE的API搜索技术 2.7.5 Windows CE缓冲区溢出流程演示第3章 Shellcode技术 3.1 Linux x86平台Shellcode技术 3.1.1 熟悉系统调用 3.1.2 得到Shell的Shellcode 3.1.3 提取Shellcode的Opcode 3.1.4 渗透防火墙的Shellcode 3.2 Win32平台Shellcode技术 3.2.1 获取kernel32.dll基址 3.2.2 获取Windows API地址 3.2.3 写一个实用的Windows Shellcode 3.2.4 渗透防火墙的Shellcode 3.3 AIX PowerPC平台Shellcode技术 3.3.1 学习AIX PowerPC汇编 3.3.2 学写AIX PowerPC的Shellcode 3.3.3 远程Shellcode 3.3.4 遭遇I-cache 3.3.5 查找socket的Shellcode 3.4 Solaris SPARC平台的Shellcode技术 3.4.1 Solaris系统调用 3.4.2 得到shell的Shellcode 3.4.3 Shellcode中的自身定位 3.4.4 解码Shellcode 3.4.5 渗透防火墙的Shellcode第4章 堆溢出利用技术第5章 格式化串漏洞利用技术第6章 内核溢出利用技术第7章 其他利用技术第8章 漏洞发掘分析第9章 CGI渗透测试技术第10章 SQL注入利用技术附录A 网络安全英文术语解释参考资料

#### 媒体关注与评论

本书作者均来自专注于网络安全技术的著名站点XPOCUS，Xcon是由XFOCUS TEAM组织的民间信息安全年会，其宗旨是创造自由、交流、共享、创新的学术气氛，促进信息安全技术的发展。  
第一届Xcon都是新的超越，我们期待与您相会。

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>