<<木马技术揭秘与防御>>

图书基本信息

书名：<<木马技术揭秘与防御>>

13位ISBN编号：9787121134715

10位ISBN编号：7121134713

出版时间：2011-9

出版时间：电子工业

作者：赵玉明

页数：240

<<木马技术揭秘与防御>>

内容概要

《网络安全入门与提高:木马技术揭秘与防御》以microsoft visual c++ 6.0
为编程工具，全面介绍了c/c++语言网络编程和socket编程的基本方法。
重点剖析了目前流行木马的编程方法，揭露了黑客木马编程技术内幕。
本书的特色在于从整体入手，先介绍木马程序的整体框架雏形，然后一步一步地深入分析木马常用的隐藏技术、管道技术、反弹技术、内核级rootkit技术、钩子（hook）技术及远程注入技术等，全书结合众多生动案例，环环相扣，多种编程方法对比分析，深入浅出，使读者既能够从中领悟到一些编程技巧，而且还可以根据这些案例进行研究。
书中提供的案例都经过作者编译通过，完整无误。

《网络安全入门与提高:木马技术揭秘与防御》适合网络管理人员及其他相关领域的专业技术人员、管理人员阅读，也可作为高等院校相关专业的教学参考书。

<<木马技术揭秘与防御>>

书籍目录

章节摘录

版权页：插图：3.载入内核阶段在这一阶段，ntldr会载入windows XP的内核文件Ntoskrnl.exe，但这里仅仅是载入，内核此时还不会被初始化。
随后被载入的是硬件抽象层（hal.d11）。
硬件抽象层其实是内存中运行的一个程序，这个程序在Windows XP内核和物理硬件之间起到了桥梁的作用。
在正常情况下，操作系统和应用程序无法直接与物理硬件打交道，只有Windows内核和少量内核模式的系统服务可以直接与硬件交互。
而其他大部分系统服务及应用程序如果想要与硬件交互，就必须通过硬件抽象层进行。
硬件抽象层的使用主要有两个原因：第一，忽略无效甚至错误的硬件调用，如果没有硬件抽象层，那么硬件上发生的所有调用甚至错误都将会反馈给操作系统，这可能会导致系统不稳定，而硬件抽象层就像工作在物理硬件和操作系统内核之间的一个过滤器，可以将认为会对操作系统产生危害的调用和错误全部过滤掉，这样直接提高了系统的稳定性；第二，多平台之间的转换翻译，这个原因可以列举一个形象的例子，假设每个物理硬件都使用不同的语言，而每个操作系统组件或者应用程序则使用了同样的语言，那么不同物理硬件和系统之间的交流将会是混乱而且很没有效率的。
如果有了硬件抽象层，等于给软／硬件之间安排了一位翻译，这位翻译懂所有硬件的语言，并会将硬件说的话用系统或者软件能够理解的语言原意转达给操作系统和软件。
通过这个机制，操作系统对硬件的支持可以得到极大的提高。

版权说明